Cybersecurity

and Safeguarding Electronic Transactions in the Pacific Islands

OCTOBER 2019

ADB Australian Aid European Union JICA NEW ZEALAND Aid Programme WORLD BANK GROUP

This report is published by the Pacific Region Infrastructure Facility (PRIF), a multi-development partner coordination, research and technical assistance facility that supports infrastructure development in the Pacific. PRIF member agencies: Asian Development Bank (ADB), Australian Department of Foreign Affairs and Trade (DFAT), European Investment Bank (EIB), European Union (EU), Japan International Cooperation Agency (JICA), New Zealand Ministry of Foreign Affairs and Trade (NZMFAT), United States Department of State (USDoS) and the World Bank (WB).

The PRIF would like to thank the governments of all participating countries for their extensive inputs, without which this study would not have been possible. We also wish to thank the authors, Chapman Tripp in association with Deloitte and Solutions Consulting House, who worked under the supervision of Michel Dorval, Technical manager of the facility, and the PRIF agencies experts who kindly provided guidance during the study.

PRIF Coordination Office, c/- Asian Development Bank
Level 20, 45 Clarence Street, Sydney, New South Wales, Australia, 2000
Tel: +61 2 8270 9444 Email: enquiries@theprif.org Website: www.theprif.org

Acronyms and Definitions

AFP	Australian Federal Police, Australia
APNIC	Asia-Pacific Network Information Centre
Budapest Convention	Council of Europe Convention on Cybercrime, CETS No 185
ccTLD	Country Code Top-Level Domain
CERT	Computer Emergency Response Team (also known as a CSIRT, a Computer Security Incident Response Team)
Convention on the Rights of the Child	United Nations Convention on the Rights of the Child, UNTS 1577
CTO	Commonwealth Telecommunications Organisation
Cyber Safety Pasifika	A cyber awareness-raising programme developed by the AFP, working with the PICP
DFAT	Department of Foreign Affairs and Trade, Australia
FBI	Federal Bureau of Investigation, United States
ICANN	Internet Corporation for Assigned Names and Numbers
ICB4PAC	Capacity Building and ICT Policy, Regulatory and Legislative Frameworks Support for Pacific Island Countries, a project undertaken in 2013 by the ITU, in association with PIFS, SPC, PITA, PIRRC and USP
ICT	Information and Communications Technology
INTERPOL	International Criminal Police Organisation
ITU	International Telecommunication Union
ITU-IMPACT Initiative	International Multilateral Partnership Against Cyber Threats, a partner of the ITU
Optional Protocol on the Sale of Children, Child Prostitution and Child Pornography	United Nations Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography, UNTS 2171
PacCERT	Pacific Computer Emergency Response Team, previously headquartered at USP (and now defunct)
PaCSON	Pacific Cyber Security Operational Network
PICP	Pacific Islands Chiefs of Police
PICISOC	Pacific Islands Chapter of the Internet Society
PIFS	Pacific Islands Forum Secretariat

PILON	Pacific Islands Law Officers' Network
PIRRC	Pacific ICT Regulatory Resource Centre, funded under the World Bank's Pacific Regional ICT Regulatory Development Project
PITA	Pacific Islands Telecommunications Association
PRIF	Pacific Region Infrastructure Facility
PTCCC	Pacific Transnational Crime Coordination Centre, an institution of the PTCN
PTCN	Pacific Transnational Crime Network, an initiative of the PICP
SFO	Serious Fraud Office, New Zealand
SPC	Secretariat of the Pacific Community
UNCITRAL	United Nations Commission on International Trade Law
UNCTAD	United Nations Conference on Trade and Development
Uniform Domain Name Dispute Resolution Procedure	A process for the resolution of internet domain name registration disputes, created by ICANN
USP	University of the South Pacific

Introduction

Context

The Pacific Region Infrastructure Facility has identified a critical need to assess the environment for cybersecurity and electronic transactions across the Pacific region, and develop an action plan.

Governments and development partners across the Pacific have been investing in telecommunications and ICT reforms and infrastructure. To maximise the benefit of these reforms and the new infrastructure, national legal and regulatory frameworks should promote confidence and trust in a broadband-enabled, digital economy.

The Pacific Region Infrastructure Facility has engaged Chapman Tripp, together with Deloitte and Solutions Consulting House, to consider the legal and regulatory frameworks supporting cybersecurity and e-transactions in the Pacific, identify potential gaps, and recommend possible reforms in participating countries.[1] We have also undertaken a regional cyber risk assessment, led by Deloitte, for the purpose of understanding the current and potential impact of cyber incidents in the Pacific and prioritising initiatives to mitigate these risks.

We intend the Cyber Risk Assessment and the Policy and Legal Gap Analysis to inform discussions within and between participating countries, donor agencies, and other stakeholders on the development of cyber and electronic transaction frameworks.

Previous reports and consultations

In January 2018, we prepared a Best Practice and Mapping Report, which identifies the building blocks for a regulatory framework enabling a digital economy at the initial, established and sophisticated stages.

We then conducted a desktop review of relevant legal and regulatory frameworks in each participating country, assessing each component against the relevant international best practice scale. Our research during this phase of the project primarily drew upon publicly available legislation, regulation and policy documents, as well as previous reports on cybersecurity and e-transaction frameworks in the Pacific. Previous reports from the ITU and PILON were particularly relevant and helpful. Alongside this, Deloitte conducted a desktop review of publically available information on existing initiatives, cyber maturity on a country and regional level, previous incidents and other reporting on cyber security and risk for the region.

From these desktop reviews, we prepared a Gap Analysis and Preliminary Observations Report, as well as a working draft framework for the Regional Cyber Risk Assessment in March 2018. These reports provided a basis for discussions with officials from each participating country about their country's existing legal and regulatory framework, cyber capability/maturity and existing risk. To enable discussions with these representatives and as part of the project outreach, we have undertaken consultation visits to:

- Tonga (4 – 5 April 2018);
- the Cook Islands (8 – 10 May 2018);

[1] The participating countries are Cook Islands, FSM, Fiji, Kiribati, Marshall Islands, Nauru, Niue, Palau, PNG, Samoa, Solomon Islands, Tonga, Tuvalu, and Vanuatu.

- Samoa (15 – 16 May 2018);
- the Solomon Islands (5 – 8 June 2018);
- Fiji (12 – 13 March 2019);
- the Republic of the Marshall Islands (19 – 21 June 2019); and
- Vanuatu (2 – 4 July, 2019).

From 13 to 15 June 2018, at side meetings to the PILON regional cybercrime workshop in Tonga, we met with representatives from the Federated States of Micronesia, Kiribati, Niue, Palau, Papua New Guinea, the Republic of the Marshall Islands, Tuvalu and Vanuatu. These meetings provided an opportunity for outreach to the various stakeholders, and enabled us to gather useful information on cybersecurity legal and regulatory frameworks in different jurisdictions, as well as ongoing cybersecurity initiatives and previous incidents.

Part A

Cybersecurity and Safeguarding Electronic Transactions in the Pacific Islands

Cyber Risk Assessment

Contents Part A

Cybercrime is becoming a greater risk when doing business in Asia-Pacific (APAC) as compared to North America and Europe. Rapidly growing connectivity and the accelerating pace of digital transformation expose the APAC region, and make it particularly vulnerable to cyber exploitation.

- Marsh & McLennan Companies, "Cyber Risk in Asia-Pacific"

Executive Summary

Background and Introduction

This Cybersecurity Assessment document provides a view of the key cyber risks for the Pacific Island regions and the 14 countries of the study which include Cook Islands, Fiji, FSM, Kiribati, Marshall Islands, Nauru, Niue, Palau, PNG, Samoa, Solomon Islands, Tonga, Tuvalu and Vanuatu.

This Cybersecurity Assessment should be read in conjunction with the Policy and Legal Gap Analysis provided in Part B.

Approach

In summary, the cyber risk assessment and the regional recommendations have been developed through a combination of:

- Seven in-country visits during April 2018 – July 2019
- A regional workshop
- Desk-based research

Full details of our approach and research sources can be found in the sections: Scope and Approach, and Research sources.

Key Insights

We have identified a number of relevant insights that will be important as a means to framing up effective recommendations and action plans. A few key ones are set out below (further detail is provided directly below under "Detailed Insights"):

1. **The cyber risk is real and growing, and the current need to address this risk is critical.**
   The Pacific Region is highly exposed to a range of cyber threats, spanning from email fraud, ransomware and card skimming to cyber bullying and child pornography. This has already affected countries both financially (impacts and losses from cyber crime stretch into the millions of US dollars) and has caused harm to the physical and mental well-being of citizens. This risk is growing rapidly with greater connectivity and more systems and information being moved online.

2. **Financial losses through fraud/scams, and the protection of children from cyber bullying and exploitation are the highest current realised cyber risks for the region.**
   We were informed of numerous cases of significant cyber fraud involving government and business email compromise or imitation, and the subsequent creation of fake payments/invoices. The cyber fraud events we were informed of totalled into the millions of US dollar, including some single events of US$300,000 or higher. In addition, cyber bullying was noted by many Pacific stakeholders as the highest existing cyber risk – in particular – severe bullying, revenge porn and objectionable materials posted on social media.

3. **There is a low level of cyber security maturity across the region.**
   The rise in cyber security risk for the region is relatively recent on a global scale. This is due to the rapid increase in connectivity and use of online services that has been stimulated by the

installation of fibre-optic broadband submarine cables for a number of participating countries. Building awareness at a senior level and creating a country-level mandate (with the appropriate regional level support and initiatives) to uplift cyber security will be critical to enabling participating countries to take advantage of the social and economic benefits of being connected. This maturity gap needs to be addressed to reduce losses and harm as a high priority.

4. **Any initiatives in the region should be linked up with existing workstreams and focus on local ownership, bilateral opportunities and building local capability.**
   There have been a number of initiatives targeted at uplifting cyber security in the Pacific, however a number of these initiatives have failed or had a restricted impact. Traditionally, the approach has not been linked up between various donor agencies, regional governments and partners. Specifically, we believe the following are key elements to a successful initiative for cyber security:
   - Take advantage of existing forums and initiatives, as opposed to creating overlaps with new initiatives.
   - Focus on bilateral opportunities that enable governments in the region to share technology, resources and templates.
   - Local ownership, skills development, documentation and operational funding are critical to long-term success.
   - Secondment and hands-on training are significantly more valuable than shorter (circa 1-5 day) classroom sessions.
   - Procurement of technology should be linked up across countries (to share skills), include cyber security requirements and should be driven by local needs.
   - Consider, but do not be limited by regional alignment and context.

We have identified numerous initiatives that have been or are still being supported in the region. Based on our research and the experience gained locally and internationally during these projects, a number of regional challenges have been identified and should be considered to continually improve the effectiveness of new projects and initiatives. Some of these challenges are:

- **Difficulties in achieving sustainability and ongoing support.** While there have been a number of useful initiatives undertaken in the region, we have observed a number of instances where insufficient ongoing support and investment have reduced their effectiveness. For example, the PacCERT initiative, and additionally a number of local initiatives related to new tech platforms and cyber strategies and legislation.
- **A lack of visibility and coordination of cyber-relevant programmes in place.** This has made it difficult for cyber related investment to be efficient and effective.
- **A large portion of attempts to reduce Cyber risk rely heavily on taking a pan-region approach.** It has been difficult to attract ongoing support and investment in regional investments. Stakeholders in the participating countries we met have specifically requested support for domestic initiatives and regional information sharing/co-ordination rather than larger scale regional initiatives. Notwithstanding a need to consider bilateral opportunities and pooling regional resources, incident reporting/information and training opportunities – our observation has been that each country has their own strong independent identity and cultural context and some projects will be more effective when they are executed within these local contexts.

Key Risks

The participating countries identified in the Pacific region face significant risk from a cyber attack or major incident. For the purpose of this assessment, we established and assessed the region against 14 key types of cyber risks that the Pacific Region currently faces across 4 harm areas, which are outlined in the table below.

The risks below have been rated based on their potential impact and likelihood.

Economic	Facilitation of international money laundering and funding of terrorism	Financial harm due to fraud or unauthorised access to banking	Inability to process or receive international payments	Inability to meet international standards for e-transactions (i.e. PCI)	
Safety and Wellbeing	Facilitation of the creation, transmission or sale of objectionable or pirated material (i.e. child exploitation)	Harm to individuals due to identity theft, cyber bullying or blackmail			
Disruption	Business disruption and/or impact to wellbeing due to critical infrastructure outage	Inability to facilitate secure and reliable communications channel for international relations/business	Destruction or ransom of information	Malicious altering or defacement of Government information	Interruption to logistics/travel
Trust and Reputation	Facilitation of global cyber attacks originating from the Pacific	Theft of intellectual property, personal information or sensitive data	Driving a malicious political agenda through hacktivism or social media.		

Key Current Regional Initiatives

While there are a large number of regional and local initiatives that involve positive cyber security outcomes, we have outlined a number of initiatives below that we have observed to be effective, well received and sustainable in the medium term.

- **Australian Cyber Cooperation Program** – established in 2016, the program aims to "promote a peaceful and stable online environment and improve cyber resilience". Australia has increased funding for the program from $4m (2016) to $38m (to 2022) and New Zealand has committed to add further support. The program has 5 areas of focus:
    1. **International cyber stability framework:** promoting an understanding of how existing international law, norms and confidence building measures apply in cyberspace.
    2. **Cyber crime prevention, prosecution and cooperation:** strengthening legislative frameworks and institutional capacity to prevent, investigate and prosecute cyber crime.
    3. **Cyber incident response:** working with partners to establish and strengthen national and regional cyber incident response capability and coordinate and share cyber security threat information across the region.
    4. **Best practice technology for development:** advocating for best practice use of technology for development by integrating cyber security by design and respect for human rights online.

5. **Human rights and democracy online:** advocating and protecting human rights and democracy online, including freedom of expression online.

Aside from supporting PaCSON (see below), Australia have supported PNG in establishing their local CERT and National Cyber Security Centre through this program.

- **Pacific Cyber Security Operational Network (PaCSON) –** funded by DFAT's Cyber Cooperation Program (see above) and initially chaired by CERT New Zealand (established April 2018), PaCSON is a network of CERTs from 14 Pacific nations. PaCSON has been established to promote sharing and collaboration in regards to cyber incident response techniques and tooling, alongside being an open forum to discuss wider cyber security concerns. PaCSON has been well-attended and is seen as an important forum in many Pacific countries, however, initial feedback suggests that it will need to be bolstered or supported by hands-on training, MOUs to support open sharing of information, and more tangible support and outputs. We have proposed a linkage between a Regional Cyber Hub and the existing PaCSON initiative within our recommendations.

- **Cyber Safety Pasifika –** this program, led by the Australian Federal Police (AFP), focuses on awareness and baseline training for the wider community, in how to stay safe online. This was the most well-known program of work relating to cyber security in the region. In particular, the AFP trained a number of Pacific-based police officers and teachers to provide cyber outreach and awareness training to their local schools and communities.

- **Pacific Islands Law Officers Network (PILON)** – this forum is helping to build awareness, skills and information sharing for the police, legal community and judiciary in regards to cyber crime. We attended the PILON regional forum in Tonga (2018) as a means of regional outreach and information gathering, which had cyber crime as the focus.

- **Council of Europe and Australian Attorney General's Office –** have both provided legislation drafting assistance and advice to a number of participating countries in the Pacific in regards to cyber crime.

- **Pacific Islands Forum Secretariat Cyber Assessment** – the Pacific Islands Forum Secretariat performed an assessment on the current state and risk in regards to cyber security – which identified the following key areas of focus:
    - promoting and supporting Forum Members accession to the Budapest Convention;
    - sharing information on cybersecurity and cyber crime threats and trends;
    - supporting the development of national cyber policies and legislation;
    - promoting awareness and educating our people on responsible cyber behaviour; and,
    - development and strengthening of Computer Emergency Response Team (CERT) capacities (national and regional).

Proposed Action Plan

To support the Pacific Region to better respond to the cyber risks identified through our analysis, there are 7 key recommendations that can be implemented.

(See overleaf)

Activity	Priority	Investment Level
1. Cyber Governance and Strategy Model **Issue:** Difficulties identifying and engaging with local representatives, alongside varying approaches to the governance of Cyber. **Solution:** A consistent set of key roles and a high-level operating model and strategy template/guidance should be developed for Cyber in each country within the region, alongside appropriate briefing pack/s with relevant information for senior Government officials.	**High**	**Medium**
2. Pacific Regional Cyber Hub **Issue:** Disparate sources of information on Cyber and related activities, alongside an immediate need for advanced technical capability and hands-on training for the region. **Solution:** Linking to and building upon the successful baseline established by the PaCSON forum for cyber security, the Regional Hub should be an iterative project to consolidate knowledge, training and capability. While initially a website would be beneficial to provide a single portal for Cyber in the region, a physical, staffed entity which owns templates and guidance, provides advanced cyber response support, performs vulnerability testing, and most importantly offers secondment opportunities for local cyber professionals to build their skillset. The Regional Hub should also provide a response capability for online child safety concerns (i.e. linkages to social media for removing offensive content).	**High**	**High**
3. Cyber Crime Legislation and Enforcement Capability Building **Issue:** Insufficient capability within law enforcement and judiciary to support cyber crime investigation and prosecution, alongside a lack of fit-for-purpose legislation. **Solution:** Targeted and ongoing awareness building and training for the enforcement, investigation and legal response to cyber crime throughout the region.	**High**	**Medium**
4. Uplift National CERT Capabilities **Issue:** A number of participating countries are establishing CERT capabilities but the lack of consistency in their role reduces their effectiveness and ability to share information. **Solution:** A template/model for local CERT and/or Cyber response functions, alongside financial and resource support for execution and ongoing operation.	**Medium**	**Medium**
5. Security Requirements for Critical Infrastructure **Issue:** There are a number of industrial control systems in use to manage critical infrastructure (i.e. controlling power, chemicals in the water supply and telecommunications), however international standards are not achievable and a fit-for-purpose approach for the region does not exist. **Solution:** A minimum set of security requirements and associated guidance for critical infrastructure providers which is focused on real regional risk and capability.	**Medium**	**Low**

Activity	Priority	Investment Level
6. Pacific Cyber Innovation Fund (Centralised Procurement) **Issue:** Donor-led projects are often executed in isolation of each other, and opportunities to leverage existing initiatives, and importantly learnings from failed/previous initiatives, are not realised. **Solution:** A platform to improve procurement outcomes and enable local and international entities to request funds for specific tactical or targeted cyber projects, including requirements for these projects.	**Low**	**High**

Detailed Insights

We have framed the following key insights through our work with a view to providing important regional context relevant to cyber risk in the region, as well as, being designed to support the successful implementation of recommendations.

The overall positive impact of connectivity to wellbeing and the economy of Pacific Island participating countries should not be understated. This is evidenced by demand – including exponential year-on-year growth of data consumption throughout the region, especially in the young generation.

This connectivity has huge benefits to individuals - enabling learning (both international and local), access to international employment opportunities, entertainment, and stronger links to family abroad. In addition, the positive social and economic impacts of this connectivity are visible – enabling international business/transactions, reliable and efficient methods for business and communication, and making local knowledge and information available to potential investors, visitors and tourists.

1. **The cyber risk to the region is real and growing, and the current need to address this risk is critical.**
   The Cyber risk to the region is real and through our work we have been privy to the types of cyber incidents that the participating countries have experienced or are currently facing. These span:
   - Financial harm - e.g. business and government email compromise and associated fraud, card skimming, unauthorised access to online banking, toll call attacks, fake online businesses targeting tourists, and scams that involve sending money overseas.
   - Disruption of system resilience - e.g. internet outages due to denial of service, data loss from ransomware, blacklisting of government services/websites due to malicious activity that is coming from them, isolated incidents of power outage due to operational (potentially non-security related) issues with industrial control systems.
   - Severe harm to the well-being of people - e.g. there have been cases of child or revenge pornography being created and/or distributed, severe cyber-bullying and harassment, Facebook account hacking, fake profiles imitating prominent figures and institutions, and defamation on social media.
   - Reputational harm – e.g. theft of private or confidential information from Government and private entities (and subsequent release).

   As a measure for relative importance, the attacks we have been informed of involving financial losses include cyber-fraud related theft totalling millions of US dollars (there have been individual fraud cases of US$300,000 – US$800,000). Based on our experience as cyber incident responders, these fraud attacks are currently becoming more frequent and advanced in their methodologies on a global and regional scale.

   Cyber criminals are not restricted by geography. Our experience has shown that attackers are most likely to perform large scale untargeted attacks against entities that have poor controls, as opposed to specific targeting of businesses that may have a high pay off. This means that immediate action to assist in managing cyber security risk is critical to participating countries in the Pacific.

   Many of these countries are improving their connectivity and pushing towards eGovernment and online payment services. For example, online transactions are increasing and for some countries, having secure payments is critical because their economies are highly reliant on international remittances and tourism. Also, critical infrastructure systems such as those used to manage and control large industrial systems (such as the power grid), that can be managed remotely over the internet, are now increasingly being targeted by malicious parties and are therefore open to significant levels of potential abuse. In

many cases, attackers are looking for "training grounds" to test malware and attack vectors before targeting more advanced entities.

Cyber risk continues to grow on a global scale – with reported and insured losses increasing year-on-year. The speed of growth for Cyber risk will be higher for the Pacific region, as connectivity increases exponentially and participating countries (with support of donor agencies) drive rapid adoption of online services and eGovernment – currently with minimal security oversight or capability.

For participating countries and local SMEs that have an interest in Cyber, the awareness of risk is focused around the individual and financial impacts. There is limited awareness of the risks to overall resilience and critical infrastructure. The Pacific region can also be seen as a "soft spot" and therefore targeted by global attackers as a target (e.g. child exploitation) or a jump off point for attacks against other countries.

Currently, there are also limited local expectations for privacy and the protection of intellectual property, however we expect this will increase quite suddenly as technologies like social media collect and use more local data. This could also cause a sudden shift in local sentiment about expectations pertaining to data protection and privacy – as seen in a number of more developed countries.

2. **Financial losses through fraud/scams, and the protection of children from cyber bullying and exploitation are the highest current realised cyber risks for the region.**
   While low maturity in the region creates significant exposure to cyber harm across the board, the focus of this assessment was to identify real current risk that is having a tangible impact on countries in the region. Those real current impacts are financial, and separately to children and young people who have rapidly grown a large online presence. Some examples are:
   - Business email fraud – we identified or heard about a large number of cases, totalling millions of US dollars, where money had been extracting by attackers either breaching or imitating email addresses, and sending fake invoices for payment. In some cases these attackers would gain access to multiple accounts and approve their own transactions via email. This was prevalent in nearly every participating country, and often targeted at Government.
   - Access to online banking and credit card skimming – we identify a number of active or past cases where attackers (including foreign visitors) had installed credit card skimmers and/or used stolen credit cards on local ATMs to extract money. There were other cases where bank employees and/or attackers had gained access to local online banking accounts and extracted money.
   - Cyber bullying – many Pacific stakeholders noted this as the highest current impact in regards to cyber crime. There were numerous active or past cases, in particular "revenge porn" or objective material being posted on social media. There is a lack of local capability in many countries to assist with these cases. The impact of these crimes can be extreme, including anecdotal stories of suicide, emigration and severe social/reputational harm.
   - Child exploitation / pornography – this may stem from cultural and/or local differences in the commonality of these crimes for participating countries, but is compounded by the growing use of social media (especially Facebook) and the immaturity of local police, parents, teachers and other professionals to combat these crimes. International support in this space is more readily available, but there is a local need for self-service guidance (see New Zealand's Netsafe program) and appropriate legislation to confirm all enforcement and legal avenues are available when it occurs.

   Additional cyber risks (especially to critical infrastructure and valuable/sensitive information) will continue to increase as these countries become more connected, collect more information, and invest in infrastructure.

3. **There is a low level of cyber security maturity across the region.**
   The majority of the participating countries have low awareness and maturity across Government in regards to cyber security risk. This is likely driven by mixed priorities and a lack of awareness at a senior

Government level, and therefore the lack of an overarching mandate to manage cyber risk. In many countries, this means that there is no strategy or work plan to uplift cyber security, and key roles and institutions have not been established/defined.

We observed that countries with a strategy, institutional leadership, appropriate legislation, and/or a local CERT were typically more mature in managing cyber security risk – but also more aware of the gravity of the work ahead of them to protect their people, information, finances and critical systems. Broadly speaking, we found the understanding of cyber security risk was stronger at the operational levels, and there would be benefits to providing fit-for-purpose briefing information to senior Government (macro) and key ministers (specific risk to their portfolio) as a part of uplifting governance.

There are strong pre-existing relationships between countries in the region, as each country faces similar challenges. As such, there is value in executing regional initiatives – especially when they deliver value and opportunities on a country-level. There are a number of region-wide cyber initiatives that have been effective and seen as valuable. These include:

- The Australian Cyber Cooperation Program – a major programme of work funded by the Australian Department of Internal Affairs (with support from the New Zealand Government). This initiative focused on establishing international frameworks, cyber crime prevention and legislation, cyber incident response, freedom of online speech and technology good practice. It is supported by more than AUD$34m in funding out to 2023.
- The Pacific Cyber Security Operational Network (PaCSON) - established on 30 April 2018, as a network of government-designated cyber security incident response officials from across the Pacific. This is funded out of Australia's Cyber Cooperation Program and has been well received with operational cyber security professionals in the region.
    - There is a desire to see this initiative expanded to include hands-on training, MOUs for information sharing and more – see our Pacific Cyber Regional Hub recommendation.
- The Cyber Safety Pasifika Program – which has involved cyber training for police, teachers and students). The focus of this program is to help young people stay safe online. It is also funded by DFAT in Australia and supported by the Australian Federal Police.
- The Pacific Islands Law Officers' Network (PILON) Cyber crime Working Group – which has helped to build awareness and skills sharing for the legal, police/enforcement and judiciary. In particular, they hosted a conference in Tonga (including the majority of Pacific Island countries relevant to this report) with a cyber crime focus in 2018.
- The Council of Europe and Australian Attorney-General's Office have both provided assistance to a number of participating countries in legislative drafting for cyber crime, and in some cases provided more broad assistance with advice, training and strategy support in regards to cyber crime.

There have also been unsuccessful projects and programs, including the now closed Pacific Cyber Emergency Response Team (PacCERT). We address factors that limit the success of projects in our next key insight below.

We also noted that many participating countries have been successful in leveraging the assistance of countries outside of the region with initiatives to help increase cyber resilience in the region. Some highlights include:

- Law enforcement from the US, Australia and New Zealand. The relationship with the FBI for the US-aligned Pacific countries has been especially effective to recover money from cyber-crime and fraud. Australia (and to a lesser extent New Zealand Police) have also been very active in building capacity, particularly in the South Pacific.
- The development of local CERTs e.g. AusCERT has been engaged to assist with the development of a Samoa CERT, and the new PaCSON initiative is being chaired by CERT NZ.
- The development of cyber crime legislation, in particular the Australian Attorney-General's Department, NZ Parliamentary Counsel Office and Council of Europe have supported legislative drafting for the development of cyber crime legislation in several Pacific jurisdictions.

4. **Any initiatives in the region should be linked up with existing workstreams, and focus on local ownership, bilateral opportunities and building local capability.**
   a. *Take advantage of existing forums and initiatives, as opposed to creating overlaps with new initiatives.*
      There are a large number of regional forums and groups supporting various initiatives and regional priorities. We found that some were well known and attended (i.e. PaCSON, PILON and Cyber Safety Pasifika), while many others were only known by a limited number of people. The large number of forums can create fatigue and confusion with participating countries, and so new initiatives should deliberately focus on bolster or linking to existing forums (even consolidating them).

   b. *Focus on bilateral opportunities that enable governments in the region to share technology, resources and templates*
      While there are a number of opportunities for regional activities, there are also specific country-level needs that would benefit from a bilateral or multi-government approach (including consider previous projects and whether a similar approach would be beneficial). Many countries across the region showed ease and willingness in regards to working with other Pacific partners, and a joined up approach could reduce costs and reliance on international support. For example, using the same technology solutions and/or templates in multiple countries will enable the sharing of knowledge and skills without needing specific international vendor support.

   c. *Local ownership, skills development, documentation and operational funding are critical to long-term success.*
      Initiatives are significantly more effective in the medium term is they build local ownership and skills. An example of this is Cyber Safety Pasifika, where the AFP train local police officers and teachers to be able to teach basic cyber hygiene and safety tips with local students and communities, as opposed to traveling to these communities themselves. In contrast, PacCERT was largely removed from participating countries (aside from updates) and local value was limited, therefore they were not prepared to fund it. In addition, we observed a number of projects where systems were no longer supported due to a lack of local skills and documentation. All projects executed by international donors should have local ownership/involvement, and sustainability through operational funding as a key requirement.

   d. *Secondment and hands-on training are significantly more valuable than shorter (circa 1-5 day) classroom sessions.*
      While a number of cyber security training options exist through various channels (there is also an opportunity to consolidate per our recommendations), these training sessions are often aimed at an audience with broad maturity and are generally covering only surface elements. There is a strong local desire for real international/local secondment opportunities which create hands-on skills that can be bought home.

   e. *Procurement of technology should be linked up across countries (to share skills), include cyber security requirements and should be driven by local needs.*
      Many Pacific Islands countries will find it easier to access skills from another regional partner than from an international contractor. In cases where systems are effective locally in participating countries, there is a desire from other countries to use those systems instead of building something new. In practice, Pacific stakeholders consistently told us that technology procurement was largely driven by donor agencies (or their consultants) who would sometimes select a product they knew, as opposed to a product that was the right local fit. There is an opportunity (see our recommendations) to consider more centralised procurement and involve local experts in the design/select phase.

      In addition, a number of technology projects (ranging from local databases/systems to industrial control systems for power) do not appear to include appropriate security requirements. Based on a

lack of local capability, it will be critical to include appropriate security controls within the design and build phase of these projects, as it is unlikely (and more costly) to be addressed at a later date.

f. *Consider, but do not be limited by regional alignment and context.*
Culturally, each participating country has a very different local context. Therefore, any proposed initiative in the Pacific region should consider these differing local contexts and how best to optimise implementation for the region. These should not be seen as a reason not to execute regional initiatives, but rather consideration should be given to balancing "one-size-fits-all" templates and guidance, and to providing training and consulting to each country individually (even in a group setting).

Furthermore, for cyber incident response and other ongoing partnerships, we recommend considering alignment (based on history and geographical location):

US Aligned

Marshall Islands, Palau and Federated States of Micronesia

Have laws and partnerships that align with US, including support from entities such as the FBI.

Australia / NZ aligned

Samoa, Tonga, Cook Islands, Niue, Tuvalu, Kiribati, Nauru, Vanuatu, PNG, Solomon Islands and Fiji

Collaborates well with, in particular: DFAT, MFAT, CERT NZ, AusCERT, Australian Federal Police and NZ Police

Scope and Approach

The Purpose of this Cyber Risk Assessment

Deloitte New Zealand, in conjunction with Chapman Tripp and Solutions Consulting House, have formed a view of the key cyber risks for both the Pacific Island region and the select participating countries as defined by the PRIF:

- Cook Islands
- Federated States of Micronesia (FSM)
- Fiji
- Kiribati
- Republic of the Marshall Islands
- Nauru
- Niue
- Palau
- Papua New Guinea (PNG)
- Samoa
- Solomon Islands
- Tonga
- Tuvalu
- Vanuatu

Through extensive desk-based research (*see Research Sources*), a regional outreach workshop, phone-based discussion with regional representatives and seven in-country visits (*completed through April – July 2019*), we have aggregated a macro understanding of the current state of regional and country-level cyber security initiatives, policies, institutions, legislation, engagement, awareness, enforcement and cyber incident response, access to capability, and connectivity. In the rhetoric of traditional risk management, we describe these factors as "controls".

This Cyber Risk Assessment quantifies the potential impact of key cyber risks, alongside the relevance and effectiveness[2] of the aforementioned controls.

This approach enables to observe:

- A broad perspective on regional and country-level risk due to cyber.
- Gaps in existing cyber security investment.
- Areas where there are opportunities to encourage or leverage regional and/or country investment.
- Existing initiatives that may provide coverage of the outcomes intended by future projects.
- Appropriate prioritisation of future investment or direction based on a desire to mitigate real regional risk due to cyber.

[2] Deloitte has not validated the presence or specific effectiveness of each individual control. Effectiveness in this instance refers to the intended outcome and purpose of the described control/s only.

Approach

The key challenge that was identified in achieving our objective (gaining a broad perspective on regional cyber risk throughout the Pacific Islands' participating countries) is the difficulty in accessing accurate and relevant information and identifying the appropriate contacts for the region. This is driven by a number of factors, including:

- A lack of centralised institutions or information for Cyber and ICT, both at a country and regional level.
- Significant variation in the governance of and institutions/people responsible for Cyber in each country.
- Investment and projects are funded and driven by a number of international entities, with varying levels of coordination and communication between projects.
- Due to Cyber being a developing capability in the region, there are a large number of projects at different stages of execution.
- Many projects have not been sustainability executed, are not completed, or have not achieved their desired outcomes.
- There can be insufficient appreciation from international entities of varying cultural drivers and dynamics.

These challenges, alongside an international and local desire to invest in cyber, underpin the need for a consolidation of initiatives and high-level quantification of real risk to the region.

For this consolidation to be effective as a tool to articulate residual economic risk from cyber, and to drive investment decision-making accordingly, we established the following key requirements:

1. **Real risks to the economy and wellbeing** – the cyber risk assessment must pivot upon real economic ("business") and wellbeing-related risks due to cyber, and their respective importance. The risks should not be technical shortcomings, which may or may not result in real economic impacts to the region.
2. **Provide a framework for controls** – initiatives (which represent "controls" in terms of traditional risk management) must be categorised, so that they can be used comparatively between countries and aligned with international good practice.
3. **Assess and provide context for underlying drivers** – due to the disparate maturities between participating countries, the overarching cyber risk assessment must be driven by country-level assessments, which can be used to target initiatives to particular groups of participating countries.
4. **Consider local context** – country-level risk assessments must include local context – in particular; population, economic drivers, international connectivity, local broadband/internet uptake, and key use cases for the Internet.
5. **Capture local contacts and key institutions** – each country-level assessment must include relevant local contacts and institutions who are responsible for planning, designing and driving cyber uplifts. This enables future assessors to make updates to the risk assessment more easily.

Based on these requirements, we have taken an iterative approach which develops a baseline that can be continually developed, with a goal of reducing effort on each pass. The core steps of this process have been:

1. Conducting desk-based research to build local context, contacts and a view of known cyber initiatives.
2. Defining a set of key regional cyber risks, and identify their relative importance in each participating country.
3. Providing a baseline understanding and context to regional contacts through the Cyber Pack and Questionnaire.
4. Iterating the risk assessment through:
    a) Calls with key contacts and stakeholders (public and private sector).
    b) In-country consultations, for the larger countries and countries where there is higher awareness and has already been significant investment into Cyber (see *In-Country Consultations* for details).
    c) Directed research based on local context (see *Research Sources* for details).
5. Validating assessment with PRIF experts at final presentation meeting (24 September 2019).

As part of the project outreach, a summary of consultation activities undertaken per country is set out below:

Country	PILON[1]	Follow-up by phone[2]	Initial meeting undertaken	In Country Consultations
Cook Islands				✓
Federated States of Micronesia (FSM)	✓		✓	
Fiji	✓		✓	✓
Kiribati	✓	✓		
Republic of the Marshall Islands	✓		✓	✓
Nauru				
Niue	✓	✓		
Palau	✓		✓	
Papua New Guinea (PNG)	✓	✓		
Samoa				✓
Solomon Islands				✓
Tonga				✓
Tuvalu	✓	✓		
Vanuatu	✓		✓	✓

Notes

1 As a part of the outreach and information gathering portion of this project, we attended the 2018 Pacific Island Law Officers Network (PILON) Conference, focused on cyber crime and child exploitation, and had individual consultation sessions to share insights with attendees, and to identify a baseline and further consultation requirements.

2 Follow-up call with country representatives after the PILON conference.

Matrix of Cyber Risks and Recommendations for the Region

Fourteen key national/regional-level cyber security risks for participating countries in the Pacific are outlined in the table below. These risks are based on key economic drivers, previous incidents, desk-based review of literature, previous studies and conversations with SMEs and leaders in the region (*see Research Sources*), and our experience of how cyber risks play out in the real world and the forms of harm that result.

This section summarises regional cyber security risks and recommendations, including an overview of key insights and current state. Further detail about regional recommendations, alongside "per-country" initiatives, risks and recommendations are captured in the *Detailed Cyber Risk Assessment and Recommendations* section below. In effect, all of the regional recommendations apply to the risks below, but we have outlined where there are strong and direct linkages to reducing a specific risk.

Type of Harm	Key Risk	Insights	Current State	Relative Importance	Regional Recommendations
Economic	**Facilitation of international money laundering and funding of terrorism**	International money laundering and terrorism are global/borderless issues which are growing in sophistication due to the proliferation of connectivity and technology. Developing countries are particular targets because they may not have the appropriate legislation, regulations or capability to detect and enforce the transfer or laundering of unlawfully derived profits. Some participating countries are reliant on international remittances (in some cases as a core factor in GDP – i.e. in 2016, 20% of Samoa's GDP was from international remittance). The inability to meet international requirements (and therefore to facilitate remittance) presents a real macro-economic risk. Additionally, although we have not identified significant use/prevalence of crypto-currencies in the region; the lack of regulation and difficulty of controlling crypto-based transactions could present further risks/challenges in the future. We noted that a national cryptocurrency project has been initiated in the Marshall Islands.	• Legislation supporting Anti-Money Laundering is present in most participating countries, but we did not assess whether this is being implemented and monitored effectively. • Some enforcement and investigation capability for financial crime is present in most participating countries, and the majority of countries have an established Financial Investigation Unit to support international investigations. • Regulation covering cryptocurrencies is not present in most participating countries. • Most countries are members of various anti-money laundering and international financial crime co-operatives.	**Medium**	2. Pacific Regional Cyber Hub 3. Cyber Crime Legislation and Enforcement Capability Building

	Financial harm due to fraud or unauthorised access to banking	There were a significant number of reports of cyber fraud events involving local citizens and business, governments and telcos. The total losses have been significant (in some countries, aggregated figures totalling millions of US dollars). These are executed via email invoice fraud (sometimes through breached accounts), scam emails and access to online banking. There have been a number of large-scale card skimming operations within the region, and skimmed cards have been used en masse in some countries to extract money. In addition, attackers commonly perform attacks in which they gain access to local PABX systems to generate large volumes of toll calls – sometimes totalling more than US$300,000 in a single attack. Awareness of fraud and scam risks are low amongst the population, but higher amongst central governments.	• Cyber Safety Pasifika is helping to raise awareness across Police and communities. • Local telecommunications companies are often supporting / covering the cost of victims of fraud and PABX attacks. • Some countries have upgraded their ATM machines to prevent the use of card skims, and skimmed cards. • Some Government agencies are doing local awareness campaigns and moving to internal domains (instead of Gmail et al) to reduce the possibility of a breach / similar address being used.	**High**	2. Pacific Regional Cyber Hub 3. Cyber Crime Legislation and Enforcement Capability Building 4. Uplift National CERT Capabilities 5. Security Requirements for Critical Infrastructure 6. Pacific Cyber Innovation Fund
	Inability to process or receive international payments	Credit card saturation and local online payments via credit cards are limited across the region, although in some specific countries usage is increasing (i.e. Fiji and Vanuatu). In addition to this, most credit card portals are provided by international vendors – which helps to reduce (but not remove) risk related to these payments. Some local businesses (especially for power and water) are accepting online card payments, and this risk will increase rapidly in the future. Cryptocurrency proliferation is low across the region.	• Central banks have some core security requirements stipulated by the SWIFT network. Many are aware and in the process of compliance. • Although electronic transactions legislation does not exist in most countries, authorisation via email is widely accepted. • Many countries have resilience in connectivity through satellites (in addition to submarine cables in some countries). • The Marshall Islands have passed law enabling them to	**Medium**	1. Cyber Governance and Strategy Model 2. Pacific Regional Cyber Hub 6. Pacific Cyber Innovation Fund

			develop a national cryptocurrency. • No other legislation or regulation related to crypto has been identified.		
	Inability to meet international standards for e-transactions (i.e. PCI)	There are a limited number of local entities providing credit card payment portals / capabilities, with the exception of larger countries and (in smaller countries) power/water are often payable by credit card online.	• There was little/no local capability identified to support compliance with relevant standards.	**Low**	2. Pacific Regional Cyber Hub 4. Uplift National CERT Capabilities 5. Security Requirements for Critical Infrastructure 6. Pacific Cyber Innovation Fund
Safety and Wellbeing	**Facilitation of the creation, transmission or sale of objectionable or pirated material (i.e. child exploitation)**	Many of the participating countries identified issues with child pornography or objectionable content being transacted over social media. In a number of countries, there have been prosecutions and/or investigations into the creation and distribution of objectionable material involving minors. This includes footage and pictures released on social media. In a number of smaller countries, there is little awareness or capability to respond to these incidents (i.e. linkages with social media, parental understanding and local police capability).	• Existing laws often provide coverage to prosecute transactions/creation of objectionable material, however in some cases the punishments are minor (i.e. small fines). • The capability to investigate cyber crime, especially crimes facilitated by social media, is very limited. • Some countries have implemented basic monitoring and blocking for known objectionable websites, normally implemented by local telcos. • Some countries have built a relationship with Facebook staff in Singapore, who assist those countries (i.e. Vanuatu) in responding to incidents.	**High**	2. Pacific Regional Cyber Hub 3. Cyber Crime Legislation and Enforcement Capability Building 4. Uplift National CERT Capabilities

	Harm to individuals due to identity theft, cyber bullying or blackmail	Cyber bullying (in some cases leading to suicide and/or self-harm) has been identified as a serious issue that is facilitated by the massive proliferation of social media throughout the region. Some countries have identified a cultural resistance to reporting these issues – which indicates a need for "self-service" and anonymous guidance (including that targeted at children and parents), such as Netsafe in New Zealand. This issue was a consistent finding and noted as the most impactful result of cyber crime (notwithstanding financial losses) in the majority of countries we spoke with. In addition, there are challenges with establishing clear identities for people due to immature / non-digital record keeping alongside many people in the region using multiple names.	• There is very limited capability within local law enforcement to respond and investigate these incidents. • There are some international partnerships to consume materials such as those produced by Netsafe in NZ (used by Tonga). • The Cyber Safety Pasifika programme has been a successful project which focuses on guidance for young people to stay safe online. This includes an easy to use website with guidance, but not a response capability. • Some countries have implemented Child Protection legislation or institutions, but most are immature. • There are very few initiatives to address digital or national identities (considered a lower priority).	**High**	1. Cyber Governance and Strategy Model 2. Pacific Regional Cyber Hub 3. Cyber Crime Legislation and Enforcement Capability Building 4. Uplift National CERT Capabilities

Disruption	**Business disruption and/or impact to wellbeing due to critical infrastructure outage**	Many local power (and to a lesser extent, water) companies are utilising centralised industrial control systems to manage their physical assets. This generates real risk of physical impacts (i.e. power being turned off) from a cyber-attack. While we did not perform any technical assessment, anecdotally and based on the overall low maturity in the region, it is possible that a number of these systems are exposed to an attack. A number of stakeholders (including from the PRIF group) are investing in additional power generation and management throughout the region – and therefore it will be critical to include security requirements, design and assessment within these projects. The majority of central/reserve banks in the region utilise the SWIFT network to facilitate international payments.	• Most central banks are compliant (or in the process of compliance with) the SWIFT Customer Security Programme – which stipulates core cyber security controls. More generally, there is still a reasonable level of risk to central banks due to their immaturity and potential for massive financial harm (i.e. targeted attacks). • The security controls implemented in most critical infrastructure entities are immature (based on available information and discussions), and we have not identified any security or assurance requirements.	**High**	1. Cyber Governance and Strategy Model 2. Pacific Regional Cyber Hub 4. Uplift National CERT Capabilities 5. Security Requirements for Critical Infrastructure 6. Pacific Cyber Innovation Fund
	Inability to facilitate secure and reliable communications channel for international relations/business	Countries across the region have varying levels of international and local connectivity. Generally, on a local basis, the uptake of mobile data is increasing exponentially year-on-year while fixed line usage drops. Many markets have been opened to competition and private companies (particularly Digicel), alongside local companies, have invested in local 3G/4G mobile networks. Coverage across most countries is good or improving rapidly. International bandwidth is a function of having a submarine cable. With many countries currently connected and others with clear established plans in most cases. As a backup or alternative, many countries use the O3B satellite	• Many countries have opened their markets to competition, which has a clear positive impact on pricing and availability of bandwidth. • There is, relatively, a significant amount of technical capability within local telecommunications companies in many countries. • Many telcos are retaining forensic evidence (SMS messages, call metadata and sometimes basic browsing behaviour) to provide this when legally requested. However, clear legislation and processes for	**Medium**	1. Cyber Governance and Strategy Model 4. Uplift National CERT Capabilities 5. Security Requirements for Critical Infrastructure

		system – which is relatively affordable for basic connectivity requirements. We saw a significant improvement in quality (and price point) in countries where the telco market had been opened to competition. We also observed that the installation of a submarine cable, while critical for progression, results in a rapid change in internet usage/uptake, and therefore increases inherent risk.	this are often not established. • Some telcos are providing basic web filtering/blocking for both objectionable materials and Government requests to censor. There are not always clear processes for this. • There have been a number of denial of service attacks which impacted connectivity in some countries. These are becoming less frequent and less impactful based on additional bandwidth available.		
	Destruction or ransom of information	Many Governments are in the process of centralising data within broad eGovernment projects. The vast majority of these are focused on "on-island" datacentres – as opposed to international cloud storage/support. This presents a risk in relation to large scale data loss due to a natural disaster. This seems historically due to bandwidth limitations, alongside data sovereignty concerns – to a lesser extent. There have been reports of ransomware attacks, but the impact of these attacks – to date – has been limited. Based on low awareness and immature controls – there is a risk of ransomware attacks being successful as an ongoing risk.	• Many eGovernment projects include provisions for backups / resilience, but these are focused on local storage. • Countries have been able to remediate basic ransomware attacks with core IT teams. • Local CERT capabilities have been established in some countries. • Improvement in connectivity will drive greater trust in off-island storage.	**High**	1. Cyber Governance and Strategy Model 2. Pacific Regional Cyber Hub 4. Uplift National CERT Capabilities 5. Security Requirements for Critical Infrastructure 6. Pacific Cyber Innovation Fund
	Malicious altering or defacement of Government information	Most governments across the region have a desire to interact with their citizens via digital channels. The benefits of this (especially where populations are spread across multiple islands) are well understood.	• A significant number of core websites do not utilise SSL encryption, and have design flaws from a security perspective • There are no security or assurance requirements in	**High**	1. Cyber Governance and Strategy Model 2. Pacific Regional Cyber Hub 4. Uplift National CERT Capabilities

		There is a very low level of maturity across the web infrastructure within countries, and we can see some evidence of defacement (although limited). In many cases, online resources we tried to access were severely out of date or unavailable. Within local infrastructure, while there has been some centralisation of identity management through eGovernment projects (partially facilitated by a relatively low number of users), there are significant risks to local data still.	most countries for Government sites and infrastructure. • Local CERT capabilities have been established in some countries to assist in responding to breaches. • There have been a number of fraud events that could have utilised vulnerable websites as an attack vector. • There is no consistent approach/technology used across the region.		5. Security Requirements for Critical Infrastructure
	Interruption to logistics/travel	At this stage, the reliance on internet based infrastructure to facilitate local tourism is limited – although this will likely increase quickly over the medium term. There have been reports of some impacts to local airports based on resilience issues with power and communications (many were mitigated by practical controls at airports). There have been limited reports of other impacts to tourism based on cyber-attacks – including attackers creating websites to imitate local businesses who do not have an online presence and take money from foreigners before they arrive.	• Anecdotally, many of the airports have resilience provisions as a part of global aviation rules and expectations. • Local CERT capabilities have been established in some countries to assist in responding to incidents.	**Low**	2. Pacific Regional Cyber Hub 4. Uplift National CERT Capabilities 5. Security Requirements for Critical Infrastructure
Trust and Reputation	**Facilitation of global cyber-attacks originating from the Pacific**	There have been reports of unlicensed telecommunications operators performing "SIM Bypass" attacks within the region, skimmed cards have been used in Pacific countries to withdraw funds, and cards have been skimmed and used elsewhere. In addition, there have been some reports of attacks being traced to origins in the Pacific.	• Many local telcos are able to implement blocking for malicious IP addresses. • Some telcos are able to provide digital evidence, but few legislative requirements exist to properly establish this.	**Medium**	2. Pacific Regional Cyber Hub 3. Cyber Crime Legislation and Enforcement Capability Building 4. Uplift National CERT Capabilities

		With the increasing international bandwidth and connectivity available in the region, alongside the immaturity of local infrastructure (i.e. attackers may gain access to use it for other attackers) there is a risk that more attacks may originate from the Pacific.	• There is limited detection capability in most countries. • Local CERT capabilities have been established in some countries, but are likely under-resourced for this purpose.		
	Theft of intellectual property, personal information or sensitive data	As a general observation, public concern about privacy is relatively low across many of the participating countries. For countries closely related to the USA (such as Republic of the Marshall Islands, Palau and FSM) there are some constitutional provisions and local awareness. Many countries have reported incidents where sensitive emails/data has been leaked by insiders – mainly for political reasons as opposed to commercial gain.	• There is limited capability to adequately secure information from internal and external attacks. • Legislation for privacy is not present in the majority of countries in the region.	**Medium**	3. Cyber Crime Legislation and Enforcement Capability Building 4. Uplift National CERT Capabilities 5. Security Requirements for Critical Infrastructure
	Driving a malicious political agenda through hacktivism or social media	In many participating countries, local Governments currently do (or wish to) maintain the ability to censor and control information they deem to be counter to the public good. Many countries reported that people were driving malicious political agendas through platforms such as Facebook. In some cases, there were reports of defaced Government websites, although many were not clearly for political gain (i.e. inserting malware, or links to fake lottery pages). There have been isolated cases where local Government have blocked social media on a country-level.	• There is limited capability or established process to manage malicious commentary on social media and other foreign websites. • Relationships with social media companies have been developed in some countries, which are effective. • Many core government websites and email accounts are vulnerable due to a lack of maintenance and cyber hygiene (i.e. patching and using encryption). • There is limited capability to respond quickly and effectively to incidents (i.e. CERT).	**Medium**	1. Cyber Governance and Strategy Model 2. Pacific Regional Cyber Hub 3. Cyber Crime Legislation and Enforcement Capability Building 4. Uplift National CERT Capabilities 5. Security Requirements for Critical Infrastructure 6. Pacific Cyber Innovation Fund

Detailed Cyber Risk Assessment

Regional Recommendations

Based on our desk-based research, calls and in-country consultations during this engagement, we recommend that you consider the following initiatives, which are designed to positively impact the wider region and enable individual countries to achieve better cyber outcomes.

We recommend that the PRIF continues to develop and iterate the Regional Risk Assessment model that has been established through this engagement. This will assist the PRIF to track the completion of key initiatives, and the relative impact these are having on Cyber risk in the region. This initial assessment forms a baseline of key risks, institutions/contacts, initiatives, and recommendations but we expect that further iterations will find opportunities to further refine and quantify risks and key metrics for the region.

The recommendations are outlined in the detail below.

1. Cyber Governance and Strategy Model	Investment Level: Medium	Priority: High
What is it?	A consistent set of key roles and high-level operating model should be developed for Cyber in each country within the region. Identifying/establishing the key roles will clarify ownership and responsibilities in relation to Cyber, and better enable donors, regional and international entities to engage and fund cyber initiatives and specific training for these roles. A briefing pack should be developed that provides a relevant overview on cyber and how it impacts the country – for ministers the briefing pack should refer to risk within each portfolio (i.e. the risk of a breaches to industrial control systems for the Energy minister). A national cyber security strategy template and associated guidance for stakeholder consultation and drafting would be useful as a local deliverable/goal within this model.	
What is the risk/challenge?	An ongoing challenge that has been outlined by a number of parties who are assessing or assisting with cyber in the region is the difficulty in identifying the right parties to engage with in-country. This issue also presents itself locally in a number of participating countries with differing views in regards to ownership and governance of Cyber. In addition, we found that cyber risk management was consistently more mature in countries which had a supporting strategy that was owned and driven by the appropriate parties.	
What are the key elements?	The core elements of this initiative should be to: • Establish a high-level operating model template for Cyber for countries in the Pacific region. This should recommend a number of consistent governance and core technical roles for Cyber, alongside stipulating the types of responsibilities for each role. • The model should also set clear expectations and limitations for the resourcing of roles – i.e. which roles need to be dedicated/shared, the level within Government that is most effective for each role, and which roles can be filled by international or private-sector partners where local capability is not suited. • The model should include a national cyber security strategy template that is lightweight and directive, alongside clear stakeholder engagement and drafting guidance. This initiative could be initially promoted and shared using the network of Cyber Response professionals that has been established by the Pacific Cyber Security Operational Network (PaCSON) but be focused on the governance layer, or via the Pacific Islands Law Officers Network (PILON).	

What will it achieve?	The governance model – and having consistently applied roles within each country – will enable: • More consistent (and sustainable) ownership and therefore improve the sustainability and consistency of outcomes for Cyber projects. • A better platform for international engagement based on the ability to identify and communicate with the appropriate contacts in-country. • Facilitation of more consistent training and capacity building for specific roles/functions at a regional level. • A platform (and or guideline/structure) upon which to develop model legislation at a regional level. • Facilitation of a clear national cyber strategy which will drive measurable progress and help to structure and prioritise local and donor investment on a per country basis.

2. Pacific Regional Cyber Hub

Investment Level: High **Priority: High**

What is it?	The Pacific Regional Cyber Hub (The Regional Hub) would build upon the baseline collaboration and sharing that has been established by PaCSON (part of Australia's Cyber Cooperation Program – and also supported by New Zealand). PaCSON conferences and quarterly check-in calls are well attended by key operational cyber security resources through the participating countries in the Pacific, however feedback from members suggests that there is a need for more substantive training and assistance. The Regional Hub can be implemented following an iterative / phased approach. For example, there is an immediate need for a website to consolidate regional assessments/knowledge, in-country representatives/leaders for Cyber, training opportunities, skilled resources, and incident reports (incidents often come in waves targeting specific vulnerabilities or approaches over a 3-6 month period). Following the website, there is a critical need for operational Cyber capability – in particular to provide cyber incident response support and technical guidance for identifying exposures and implementing controls. Going forward, there will be a benefit to having a physical location (we recommend Vanuatu, Fiji or Samoa, based on location and relative capability), a resource to update the website (ongoing relevance will be key to uptake), and access to experienced cyber professionals (we suggest a mixture of internationally sourced and local initially) for various in-country or regional projects. It should not be based within an educational institution – as it must be operationally focused. The hub would be responsible for providing advanced cyber incident response support, supporting centralised incident reporting and early warning, incident and vulnerability monitoring, training and capability building, storing and distributing templates and guidance (per other sections), centrally procuring and making tools available, and providing trusted advice to Governments throughout the region. The Regional Hub's response capability must provide support to the victims or serious cyber bullying, revenge porn and exploitation – which will include creating linkages with social media companies. The Regional Hub must be established taking learnings from the previous "PacCERT" initiative. Notwithstanding that PacCERT being established in 2011, when the risk landscape for Cyber was less established (and therefore the priority for local Governments was lower), PacCERT also identified the following challenges: • Lack of operational funding – PacCERT did not have adequate operational funding, and so participating countries were asked to contribute significant funding towards it, before they had realised the value of the institution. • Education focused and not operational – many representatives we spoke to noted that it was difficult to apply or operationalise the guidance provided by PacCERT. In addition an operational cyber incident response (or other) capability that could be leveraged by members was not available. We have suggested areas above that were noted as high priority / high usefulness. • No secondment opportunities to learn hands-on technical Cyber skills – there is significant demand for "hands-on" technical training, specifically through secondment opportunities throughout the region. Staffing the Regional Hub with a mixture of international and regional representatives (including secondees) will provide a great opportunity for this training and knowledge sharing.
What is the risk/challenge?	A key challenge identified by participating countries (and ourselves) was having a holistic view of the training, capability, incidents and in-country contacts available in regards to cyber security across the region. While there are some opportunities for training, many are not well known and opportunities are difficult to compare. In addition, there is a genuine need for secondment opportunities that immerse high potential staff in real

	cyber security work – as opposed to short class-room style training. Currently, cyber incident response support is not formalised, and local experts and Government do not have a consistent and reliable support mechanism to advise them on cyber security. In addition, challenges have been identified in international contractors who deploy projects but are then not available to support them. Projects could be supported and deployed by the hub – meaning ongoing assistance is available, and local capability is established within the hub.
What are the key elements?	The Regional Hub will benefit from: • Implementation and operational funding to support at least 2 years of operation; including for core staff, technology, and premises. A commercial model that involves stakeholders should be considered, but it will be important to exhibit value in the initial period before this is implemented. • Strong linkages with and/or to potentially be a part of existing initiatives – specifically PaCSON. • Staffed to support advanced cyber incident response support and technical security assessment and monitoring. • A well-designed website which provides a clear view of and access to training available throughout the region, templates, guidance, tools and up-to-date governance level information on risk. • Secondment (which will also reduce cost) for CERT and other cyber security professionals throughout the Pacific to work within the hub and build operational cyber security skills. • Templates and guidance for cyber strategies, cyber crime legislation, security risk assessment and further needs. • Technical ICT templates for key secure services (i.e. central Government websites, webmail, payment card functionality, etc) that can be reused safely by members. • Management of information sharing agreements between countries to support open and safe collaboration on cyber security. • Linkages established with social media companies, and the appropriate capability to support victims of serious cyber bullying, revenge porn and exploitation.
What will it achieve?	The objectives of the Pacific Cyber Capability Programme (PCCP) would be to: • Provide a single point for international Cyber experts to interact with if they are looking to work / make an impact in the Pacific. • Provide a single point for Pacific participating countries to apply for and access Cyber human resources and training. • Enable sustainability by leading projects from the Regional Hub (not a sole contractor) and providing secondment-based "on the keyboard" training for local professionals. • Greater visibility, oversight, control and tracking of projects and resource effectiveness throughout the region. • Uplift the safety, ease and consistency of deploying critical eGovernment and payment services through reusable technical templates and advice. • Provide a single view on training opportunities, risk/progress, and key contacts and institutions across the region. • Have trusted (contractually and proximity) resources available to assist in major cyber incidents impacting critical institutions across the region. • Use economies of scale to assess and provide tooling to support cyber security prevention, detection and response. Consistency will drive down licensing (where applicable), procurement/assessment, and training costs. • Provide a centralised point for incident reporting, regional governance reporting and early warning systems. • Provide support to victims of serious cyber bullying, revenge porn and other forms of online exploitation.

3. Cyber Crime Legislation and Enforcement Capability Building	**Investment Level: Medium**	**Priority: High**

What is it?	In addition to supporting the development and implementation of fit-for-purpose cyber crime legislation (see associated Chapman Tripp report, "Cybersecurity and Safeguarding Electronic Transactions in the Pacific Islands"), there is a need to provide targeted and ongoing awareness building and training for the enforcement, investigation and legal response to cyber crime throughout the region. This should be supported by clear enforcement protocol/s for investigating cyber harassment, bullying and crime executed using common platforms (i.e. local SMS and mobile

	calling, Facebook, Instagram, etc). This training should include investigators, law practitioners (prosecution and defence lawyers), enforcement agencies (police, crimes unit, CERT) and the judiciary. **Key dependencies:** the effectiveness of local prosecutors and law enforcement in tackling cyber crime (and the associated impacts) will be dependent on the establishment of local CERT capabilities as outlined in **Uplift National CERT capabilities** above. National CERTs and associated capabilities outlined above will be required to identify crime and provide technical assist into investigating and remediating the actions of criminals in each country and across the region.
What is the risk/challenge?	The majority of Pacific Island nations have embarked on projects to develop and implement cyber crime legislation that is fit-for-purpose and aligned with the Budapest Convention. As an outcome of acceding to the Budapest Convention, the Council of Europe offers some training to prosecutors. However, we have identified significant gaps in awareness and the ability for local police, prosecutors, judges and other key stakeholders to understand, investigate and enforce crimes that relate to this legislation. The majority of internet traffic in the region is to social media platforms such as Facebook. We were informed of a number of cybercrimes and incidents that have taken place using these platforms (including fraud/scams, harassment, 'revenge porn', exploitation, defamation of Government and local figures, and the sale and purchase of illicit goods and images/videos). Specific training, processes and enforcement protocol that relate to this/these platforms will significant improve the ability of local entities to respond and mitigate the impact of these events.
What are the key elements?	We recommend: • Develop and implement fit-for-purpose cyber crime legislation (see Chapman Tripp's associated report for detail). • Ongoing awareness campaigns that highlight the real risk of cyber crime, the common types of attacks in the region, and the training/assistance available to law enforcement and prosecutors. • Establishing an end-to-end training programme for lawyers, prosecutors and judges in the region that focuses on the execution of cyber crime legislation based on the Budapest Convention. This may be executed through an existing conduit such as the Pacific Island Law Officer's Network (PILON). • Establishing a technical-level training programme for local police officers – which should include digital forensics, security operations / service management and cyber detection and investigation. This may be executed with support from an existing conduit such as the Cyber Safety Pasifika programme. • Developing a core enforcement and investigation protocol template for engaging with social media platforms (especially Facebook), local ISPs, and other key entities that hold evidence relating to cyber crime. Individual countries may need financial and/or technical support to effectively implement this template.
What will it achieve?	The goal of the capability and awareness building activities should be to: • Confirm there is legal coverage to support prosecutions and appropriate sentencing for cyber criminals. • Increase the local awareness and understanding of law enforcement, so that they can better engage with the community and identify/investigate cyber crimes. • Provide end-to-end training for police, prosecutors and judges to assist them in identifying, investigating and prosecuting cyber crime. • Improve the ability of local police to interact with ISPs and social media platforms to obtain digital evidence and take action against cyber criminals. • Reduce the risk of harm to children and young people who are currently exposed to exploitation, harassment, bullying, scams and 'revenge' porn. • Support the effective implementation and use of new cyber crime legislation for many of the participating countries.

4. Uplift National CERT Capabilities	Investment Level: Medium	Priority: Medium

What is it?	A number of participating countries in the Pacific have established a local Cyber Emergency Response Team (CERT) capability. These CERT teams create a local capability which is used to support both technical and advisory-based cyber security for local businesses and Government. They form a critical institution to support ongoing cyber security needs at an operational level. We suggest that a Cyber Response Framework is developed as a template for local CERT and/or response functions, including key business functions, operating model, technical platforms and an international sharing/MOU model to support real sharing and collaboration (the lack of clear Memorandums of Understanding between CERTs has been a regional challenge). This framework should outline key contacts and/or regional capabilities that can be accessed to help with region-specific issues such as malicious use of social media (child exploitation/harassment, defamation and revenge porn) and card skimming. An example would be providing a linkage to Facebook's representatives in Singapore, which a number of countries have used to assist in social media-based investigations. This initiative should also provide specific funding/resourcing which enables the donor group to provide capability into local Cyber Response/CERT functions for medium term period (i.e. 6 months to 2 years).
What is the risk/challenge?	As the Cyber threat landscape continues to increase for countries in the Pacific, there has been a regional push to uplift cyber crime legislation to provide a basis to tackle some of these threats. This legislation needs to be supported by local enforcement capability, and additionally, many of these countries do not have local resources they can fall back on for responding to and remediating cyber-attacks on critical assets. After the closure of the Pacific Cyber Emergency Response Team (PacCERT), a number of participating countries have embarked on the journey towards establishing their own local CERT capability, with a local CERT capability being outlined by most participating countries as one of their highest priorities. A CERT capability is crucial, and should be supplemented by response capabilities that help to tackle major regional issues such as child exploitation, human trafficking, card skimming and unlicensed telecommunications operators. There are good reasons to establish a Cyber response capability (i.e. a CERT) locally, including improved local context and interconnectivity, improved response times, increased trust, and improved local capability in the medium term. However, each CERT that is currently being established is using a disparate model – which means that over time it will be difficult for the CERTs them to inter-operate, and harder for each country to maximise the benefit they can get from their local capability. The investment into understanding the functions, operating model and structure of a CERT for each country is also very inefficient. Additionally, there have been difficulties funding and resourcing Cyber Response/CERT capabilities locally – which has reduced their ability to be sustainable and/or they can be ineffective due to resourcing constraints.
What are the key elements?	This initiative should include: • A template for local Cyber Response/CERT functions, including key business functions, operating model, an international engagement model. • A set of core technical toolsets which cover at least: digital forensics, vulnerability testing and management, threat intelligence and analytics, open-source intelligence (OSINT), incident management and reporting, social media monitoring and incident monitoring and detection. • A capability and training model that gives direction and structure to local resources who are looking to upskill and add value to the local CERT. • A Memorandum of Understanding template to support open incident and information sharing between country-level CERTs. • Create a linkage with and utilise the existing PaCSON network to continue to collaborate and build regional interconnectivity between CERTs. • Specialist resource augmentation to establish the core team and to provide (as needed) ongoing support.

	It will be important for this initiative to utilise and link with the PaCSON initiative (part of Australia's Cyber Cooperation Program) – to confirm it leverages and supports the baseline that has been established by PaCSON.
What will it achieve?	The Cyber Response Framework will: • Improve the ability of countries to identify and address major regional issues such as child exploitation, harassment, defamation, and human trafficking that are partially (or wholly) facilitated using social media and similar platforms. • Identify "tourist criminals" who are often responsible for card skimming and unlicensed telecommunications operations. • Significantly reduce the investment/cost for each Pacific Island country to design and implement a CERT capability. • Improve the ability of participating countries to inter-operate and share knowledge/resources between CERTs. • Improve the outcomes/effectiveness of each local CERT by establishing a view of "what good looks like". • Establish a consistent set of, preferably free and open-source, technical toolsets for CERTs – which will enable more efficient training and sharing of resources and knowledge. • Encourage and facilitate international and regional cooperation, as response protocols may be similar across the region. For example, working relationships can be formalised with Interpol, FBI and other key stakeholders / experts.

5. Security Requirements for Critical Infrastructure	**Investment Level: Low**	**Priority: Medium**

What is it?	A minimum set of security requirements (including for people, process and technology) should be developed for critical infrastructure providers in the region. This includes infrastructure that supports energy, water, central banking, eGovernment and telecommunications. Where applicable, technical ICT templates (pre-build systems or configurations) could be developed to support critical services (i.e. Government webmail, payment card sites, etc) – see the **Pacific Regional Cyber Hub** recommendation above for more detail. *** The PRIF stakeholder group should consider upcoming/ongoing infrastructure projects and whether they include appropriate security design and assessment within the project scope (i.e. the large ongoing solar power deployment assisted by the World Bank in the Marshall Islands – which includes a digital control system).**
What is the risk/challenge?	Local infrastructure providers (including for power, water, banking, eGovernment and telecommunications) are increasingly taking advantage of remote access and operational technology (industrial control systems) which enable digital-based management of their assets. While great efficiencies and rapid response can be enabled by these technologies, the nature of their increased connectivity generates new risks. These risks have been realised by a number of international entities who have been attacked (i.e. a Ukraine-based power company was attacked twice with increasing sophistication in late 2015 – causing extended power outages to over 230,000 residents), and the potential to cause broad impacts to the economy and the safety of citizens drastically increases the impact of these events. The attack on the Ukraine further reinforce that attackers may target less developed countries to test the cyber weapons they have developed for critical infrastructure. We identified a number of entities in the Pacific who were using ICS/SCADA digital control systems for critical infrastructure, and in addition were told of a number of upcoming projects to implement these systems as a part of uplifting power generation in participating countries. Separately, central banks have reacted well to the expectations of the SWIFT Customer Security Programme (SWIFT is used by banks to enable international remittances), and the security requirements outlined by this programme have been recognised and, broadly, implemented or uplifted by participating countries. There are no such requirements for critical infrastructure providers – and many that we interacted with in-country did not have any clear initiatives or an approach to uplift cyber security. There was little awareness of Cyber risk.
What are the key elements?	The security requirements should focus on securing the operational technology (as opposed to information technology) used by critical infrastructure providers to control physical assets in the region. Key elements should include:

	• Platform-ubiquitous technical security requirements (i.e. access and authentication, malware protection, patching/vulnerability management, monitoring and detection, incident response and resilience). • Staff vetting and ongoing identity and access management. • A certification and accreditation process for procuring and commissioning new industrial control systems. • Clear partnerships and plans for business continuity, disaster recovery and incident response. • Audit and/or assurance programme/s that help these entities to build confidence in the systems and services they have in place.
What will it achieve?	A baseline standard for security, which is designed to reduce the likelihood and potential impact of cyber attacks on critical infrastructure – alongside increased awareness of Cyber risk and the relative levels of maturity for each organisation.

6. Pacific Cyber Innovation Fund (Centralised Procurement)	**Investment Level: High**	**Priority: Low**
What is it?	The Pacific Cyber Innovation Fund (PCIF) would be a platform to enable local and international entities (public and private) to request funds for specific tactical or targeted cyber projects. The fund would stipulate specific requirements for funding which directly address problem areas that have been observed in previous projects (as below). A neutral entity (potentially the PRIF, or a nominee on the PRIF's behalf) would be required to administer and measure the ongoing effectiveness of the fund. In particular, the PCIF could act as a central procurement entity, which would help to reduce licensing cost (via economies of scale), reduce due diligence costs, and promote sharing of technology and skills across the region. There is potential for the Pacific Cyber Innovation Fund to be linked with or part of the **Pacific Regional Cyber Hub** outlined above.	
What is the risk/challenge?	There has been significant international investment into Cyber for the region, which has been focused on both projects executed by foreign entities and by local Government. Key challenges for these projects have been tracking outcomes, building sustainability, and both utilising and building local capability. In some situations, local entities identify high risk or tactical Cyber issues where they have a direct ability to solve these problems – but do not know how to access the skills, tooling or funding to do so. In many countries, key private and public sector organisations (i.e. telecommunications companies and local CERT teams) have significant capability, but cannot access funding to execute cyber projects. The majority of existing initiatives are supported by international donors/partners on a "push" system. There is an opportunity to create local ownership and tailor smaller projects by providing a forum and opportunity for local cyber security experts to access funding and support for specific issues that are prominent for them. In addition, we observed that there were significant opportunities (and a cultural desire) to share skills across participating countries.	
What are the key elements?	The fund should be administered by a third party (potentially the PRIF or a nominee on PRIF's behalf), must include local experts who understand context, and be discretionarily accessible to any entities who can satisfy prescribed criteria for accessing the fund – including international entities, private and public sector. It will critical to establish and measure requirements that address key regional investment issues, such as: • Clear objectives, timings and stage gates for all potential projects. • Sustainability of projects from an ongoing/operational perspective – including clear ownership. • Utilisation and development of local resources. • Developing local institutional knowledge and ownership. • Technical security requirements where a platform or service is being implemented.	

What will it achieve?	The fund would enable its administrators and donors to better utilise local capability and platforms that are established with each country (including, for example, within local telecommunications providers). It would reduce costs of procurement and technology, improve skills sharing and would enable the efficient and highly effective response to critical Cyber risks within each participating country through the development, application and tracking of specific principals that will drive better outcomes based on past experience.

Country-Level Evaluation

Through desk-based research and analysis, discussions with key contacts (both via phone and at the 2018 PILON conference - *see Appendix*), and in-country consultations (April-June 2018, see *In-Country Consultations*), we have captured key information relating to cyber security initiatives and risk for each of the 14 participating countries outlined by the PRIF.

It is important to note that due to the relative immaturity of the region, and the increasing connectivity, reach and sophistication of global attackers – all of the key cyber security risks identified are relevant to each country. Based on our work to date, we have shaded in colour the risks that we believe have the highest likelihood and potential impact for each country. This is based on the maturity of controls, and also the potential for financial, reputational or personal harm to citizens and organisations within the countries.

Cook Islands 

Key Thoughts
The Cook Islands, while not currently served by a submarine cable for international connectivity (the Manatua submarine cable will likely provide this within the next few years), have strong local connectivity and serviceable international links provided by the O3B satellite system. Anecdotally, 70% of this international bandwidth is currently consumed by Facebook and Youtube.

The Cook Islands Government has set a strategic direction to centralise and improve ICT infrastructure as a part of the National Sustainable Development Plan (2016-2020) and the e-Government Strategy (2013-2018). These documents, and the direction they set, also include provisions for improving information security and resilience. The e-Government project is owned by the National ICT Office and provides a centralised network, infrastructure, identity and core productivity applications (i.e. email) for internal Government users. It is well progressed, with a number of agencies currently using these services.

Based on its size and close ties with New Zealand, it is likely that resource to support cyber security (including incident response and enforcement) will often be sourced from New Zealand and Australia (including from Government, private sector and respective police departments). These relationships have been used in the past to address cyber security and, anecdotally, have been effective.

As high priority tasks, the Cook Islands would benefit from:

- Defining and formalising ownership of Cyber security within Government, and developing an action plan that aligns with its overarching strategies for ICT and development.
- Completing the development and implementation of new cyber crime legislation; including provisions for cyber bullying/exploitation, an enforcement protocol and requirements for the telecommunications sector.
- Formalising the international relationships and processes that support and help to build local capability in cyber incident response, and broader design, implementation and governance capabilities – especially for key entities such as the National ICT Office and Cook Islands Police.

Population:	**Key Economic Drivers:**	**Connectivity:**	**Broadband Uptake:**	**Core Internet Uptake/Use Cases:**
17,411 (2018; United Nations Department of Economic and	• Tourism. • Exportation of Black Pearls.	• International: O3B Satellite Uplink provided by Telecom Cook Islands	• Internet Users: 11,377 (2017; Internet World Stats).	• Social media (Facebook). • Video (Youtube).

Social Affairs: Population Division).	• Agriculture and Fishing • Handicrafts • International remittance and aid.	(owned by Bluesky Samoa). No submarine cable. • Local: Microwave (connecting close islands) and Spark VSAT network (outer islands). • Local: 3G (100% of Rarotonga), 2G for other islands. • Local: 10Gbit MPLS network around Rarotonga for Government use.	• Mobile: 6000 unique subscribers (2015; GSMA Intelligence).	• Telecom Cook Islands offer credit card payments online (hosted in American Samoa). • Internet Banking (provided locally by the Bank of Cook Islands).

Key Contacts:
- Minister of Telecommunications – Hon. Mark Brown.
- ICT Director for the Government of the Cook Islands (Pua Hunter).
- Attorney General – Henry Puna.

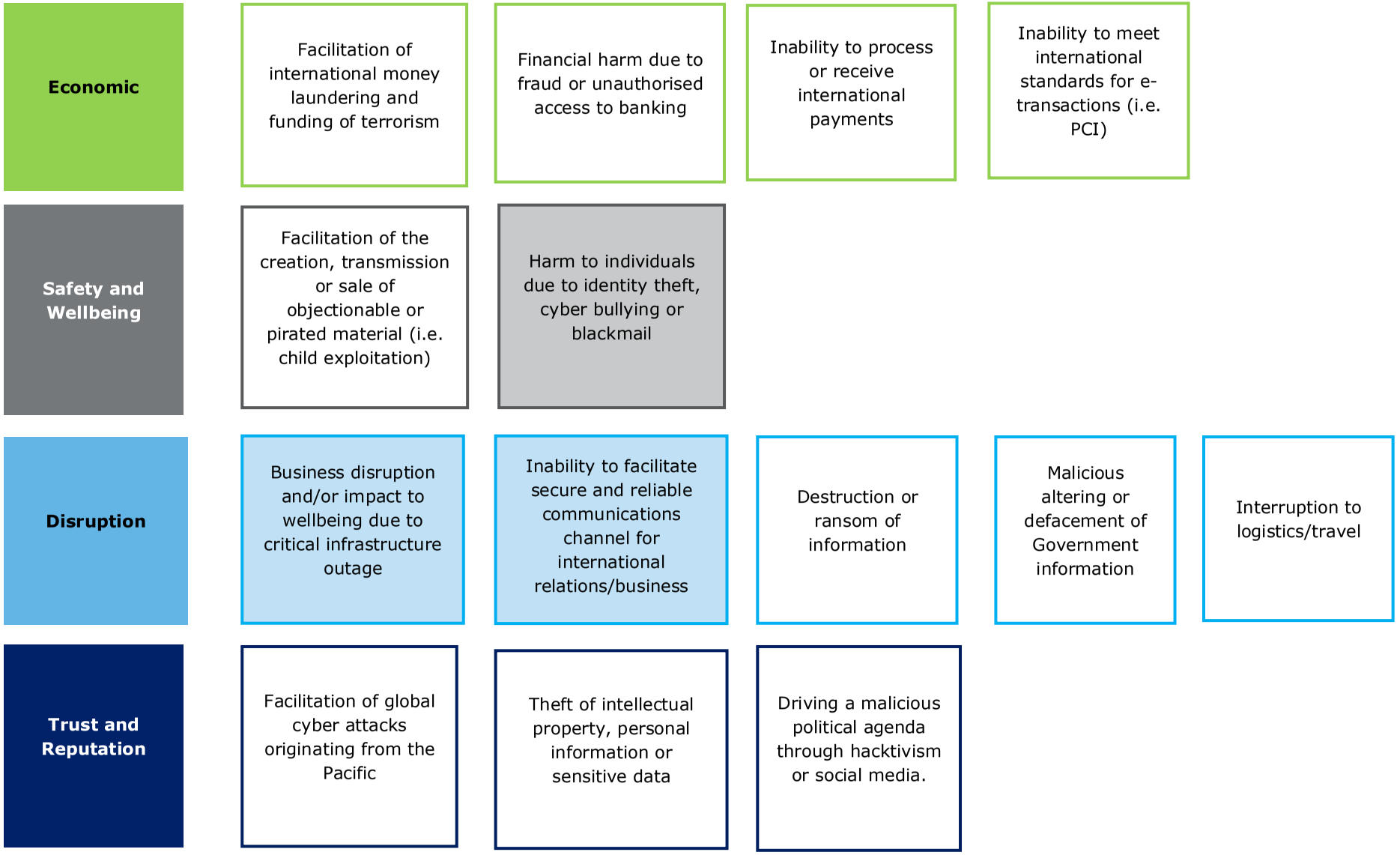
Key Institutions:
- Crown Law Office.
- Office of the Prime Minister (responsible for Central Policy and Planning, ICT, and Emergency Management)
  - National ICT Office (which includes the ICT Director).
- Ministry of Finance and Economic Management.
  - Pacific Islands Internet Society (PiciSoc) which supports the Cook Islands Internet Action Group (CIIAG) and is an arm of The Internet Corporation for Assigned Names and Numbers (ICANN).

Cyber Area	Current State	In-Progress / Planned
Strategy	**Strategy, Roadmap and Policy** • No overarching cyber security strategy. • Cook Islands National Information and Communication Technology Policy 2015-20. This policy (Section 2.3) outlines the need for improved information security for e-Government. • E-Government Strategy (2013-2018); focuses on developing basic IT infrastructure to support Government services. • The Government of Cook Islands Internet Usage Policy has been developed. • Te Kaveinga Nui, the National Sustainable Development Plan, sets out the plan to build resilient infrastructure (including for ICT). **Institutional Bodies** • National ICT Office and Crown Law Office work jointly on ICT issues, but no specific entities are in place for cyber security. **Training and Awareness** • Taking part in the Cyber Safe Pasifika Programme (cyber security training for police, teachers and students). Four police officers have been trained (May 2018) to provide this course.	• None identified to date.

	• Once a year, the Ministry of Education and BlueSky/Telecom Cook Islands (TCI) bring Microsoft training to the Cook Islands. • Cook Islands Internet Action Group (CIIAG) run community development programs to build ICT capability. **Risk Management** • A penetration test was conducted on the e-Government infrastructure by an international consultant (potentially in 2017). • No formal risk management is in place relating to cyber security.	
Secure	**Legislation** The associated Chapman Tripp analysis outlines the following: • Cybercrime (substantive) – initial. • Cybercrime (child protection) – initial. • Cybercrime (procedural) – initial. • Electronic transactions – initial. • Privacy – initial. • Data protection – none. • Digital authentication – initial. • Consumer protection – sophisticated. • Intellectual property – established. **Capability** • Some technical cyber security capability (including an international consultant) is resourced from the National ICT Office (within the Prime Minister's Office). **Requirements and Standards** • The Bank of Cook Islands is compliant with the security controls outlined by the SWIFT Customer Security Programme (CSP) as at December 2017.	• The associated Chapman Tripp analysis outlines additional legislation activities that are in-flight.
Vigilant	**International Co-operation and Intel** • Subscribe to the New Zealand South Cross Network Operations Centre (SNOC). • Member of the Pacific Islands Law Officers' Network (PILON). • Member of Pacific Cyber Security Operational Network (PaCSON). **Detection and Monitoring** • E-Government infrastructure: some basic monitoring capability has been implemented (using a Splunk SIEM) as a part of the e-Government initiative. • Telco: SMS messages are stored, alongside high-level browsing information for customers. No capability to lawfully intercept data or voice calls.	• The Bank of Cook Islands is in the process of implementing "RackFoundry" – a security monitoring and protection solution.
Resilient	**Connectivity and Redundancy** • Connectivity is available via O3B Satellite Uplink. • 4G+ launched across Rarotonga and Aitutaki in March 2017. • Telecom Cook Islands operate a disaster recovery (DR) site to support redundancy for core infrastructure, in a separate part of Rarotonga.	• Manatua submarine cable announced in 2015 which will connect Cook Islands to New Zealand and Hawaii (has been underway since 2016).

	Cyber Incident Response (CERT) • No CERT identified. **Cyber Crime Enforcement** • Australian Federal Police (AFP) has previously provided digital forensics assistance (specifically, on a phone which was involved in a child exploitation case). There is a good working relationship between AFP and the Cook Islands Police. • Country code top-level domain (CCTLD): a draft dispute resolution process has been developed, but there has not been a requirements to use it. • Financial Supervisory Commission has been established to support investigation of money laundering and the financing of terrorist activities.	• The Cook Islands will be connected to the Manatua cable system, which is due for completion in May 2020.
Previous Cyber Incidents	Our conversations with key stakeholder representatives identified a number of previous cyber security incidents based on anecdotal evidence: • Month long country-wide internet outage in 2016 due to a backup site burning down. • 7 hour power outage due to a glitch in a power company's Supervisory Control and Data Acquisition (SCADA) software. • Police have received reports from people who were victims of email based fraud/scams – these people have sent money abroad, which was not recovered. • Hacking/misuse of Facebook accounts for both children and prominent figures. • Distributed Denial of Service (DDoS) attack launched from USA-based addresses – knocking out Internet access for outer islands for less than 24 hours. • A telco was breached, and attacker made outbound calls to overseas toll numbers. This was identified and remediated quickly which reduced the financial impact. • Malware has been identified and removed from a number of staff devices – which so far has caused little known impact.	

Key Cyber Risks – Cook Islands



Federated States of Micronesia

Key Thoughts
The Federated States of Micronesia (FSM) have international broadband connectivity through the HANTRU1 cable system, and the telecommunications market has recently been opened to competition, which has driven an uptake in internet and social media use.

The Department of Transportation, Communication and Infrastructure (TCNI) is the agency response for ICT in Government, and for FSM's all-of-government infrastructure. While FSM representatives noted that TCNI was likely the lead agency for cyber security, we found no indication that this has been formalised. In addition, FSM does not currently have a cyber security strategy or cyber crime laws in place.

Privacy was outlined as a key area of concern for people in FSM, which differentiates it from most other Pacific Island countries that we examined. While no privacy laws currently exist, the representatives we met suggested that businesses and Government were conscious of what data they collect and how that data was managed – based on public demand.

During our discussions we were informed of only one incident (see incidents section below), but based on relative immaturity of cyber-related institutions, it is likely that further incidents have occurred and not reported/captured.

As high priority tasks, the FSM would benefit from:
- Developing a cyber security strategy and work plan, and confirming that there is appropriate support from senior Government officials.
- Implementing fit-for-purpose cyber crime legislation and providing training to the judiciary (and the police as required).
- Confirming telecommunications providers are mandated to retain logging information for an appropriate period (at least 1 year), to support local and international investigations.

Population:
106,227 (2018; United Nations Department of Economic and Social Affairs: Population Division).

Key Economic Drivers:
- Farming.
- Fishing.
- Mining.
- Foreign Aid. Financial assistance from the U.S. is the primary source of revenue (The United States provides over $130 million in direct assistance every year, along with a variety of federal grants and services, until 2023 https://www.state.gov/r/pa/ei/bgn/1839.htm).

Connectivity:
- International: There is a submarine cable, a HANTRU1 Cable System for international connectivity.
- International: For international redundancy there are four satellite earth stations operated by Intelsat.
- Local: Inter-island connectivity for Chuuk and Yap is provided by FSMTCable.
- Local: Other islands are connected via shortwave radio.

Broadband Uptake:
- Fixed Line: 3 per 100 inhabitants (2017; ITU).
- Mobile: 0 per 100 inhabitants (2017; ITU).
- Internet users: 56,193 in December 2017 (2017; internetworldstats).

Core Internet Uptake/Use Cases:
- Recreational.
- 21,000 Facebook users (19.9% penetration rate) (2017; internetworldstats).

Key Contacts:
- Secretary, Department of Justice – Joses R. Gallen.
- Secretary, Department of Transportation, Communication and Infrastructure – Lukner Weilbacher.

Key Institutions:
- Department of Transportation, Communication and Infrastructure (TCNI).
- Department of Justice.
- Chief Executive Council (CEC).
- State and National Leadership Council (SNLC).
- Telecommunications and Submarine Fibre Optics Task Force.

Cyber Area	Current State	In-Progress / Planned
Strategy	**Strategy, Roadmap and Policy** • National ICT and Telecommunications Policy (2012) which contains some cyber-related strategy. **Institutional Bodies** • The Department of Transportation, Communication and Infrastructure (TCNI) has been recognised as the agency responsible for cyber security. • Auditor-General's Office and the FSM Public Auditors were identified as institutions with an interest in cyber security. **Training and Awareness** • Micronesia is a beneficiary of Regulatory and Legislative Frameworks Support for Pacific Island Countries (ICB4PAC). • Takes part in the Cyber Safe Pasifika Programme. **Risk Management** • None identified to date.	• None identified to date.
Secure	**Legislation** The associated Chapman Tripp analysis outlines the following: • Cybercrime (substantive) - none • Cybercrime (child protection) – none. • Cybercrime (procedural) – initial. • Electronic transactions – none. • Privacy – initial. • Data protection – none. • Digital authentication – none. • Consumer protection – none. • Intellectual property – established. **Capability** • Digital forensics (within FSM Police). **Requirements and Standards** • None identified to date.	• None identified to date.

Vigilant	**International Co-operation and Intel** • USA Federal Bureau of Investigation (FBI) in Hawaii / Guam. • Member of the ITU-IMPACT Collaboration. • Member of the Pacific Islands Law Officers' Network (PILON). • Member of Pacific Cyber Security Operational Network (PaCSON). • Receives support from the Australian Federal Police through the Cyber Safety Pasifika programme. **Detection and Monitoring** • None identified to date.	• None identified to date.
Resilient	**Connectivity and Redundancy** • Single submarine cable providing international connectivity to Pohnpei. • Two outer islands connected by submarine cable (Chuuk and Yap) with further planned. • FSM Telecom (Single main ISP). **Cyber Incident Response (CERT)** • No CERT. • Support provided by FBI in Hawaii and Guam. **Cyber Crime Enforcement** • There is some limited capability within the FSM Police (including digital forensics). • There is no current mandate which requires local ISPs to maintain log information for investigations.	• The Pacific Regional Connectivity Project aims to connect the remaining three unconnected states of Micronesia to high-speed broadband by the end of 2019. • The FSM Police are planning to establish a cyber security crime unit – but need additional funding for staff and equipment.
Previous Cyber Incidents	Based on our conversations with stakeholder representatives, we have captured a number of previous cyber security incidents based on anecdotal evidence: • A Government email account was breached, and money was extracted using a fraudulent invoice. The FBI in Hawaii/Guam assisted with the response and some of the money was recovered.	

Key Cyber Risks – Federated States of Micronesia

Economic	Facilitation of international money laundering and funding of terrorism	Financial harm due to fraud or unauthorised access to banking	Inability to process or receive international payments	Inability to meet international standards for e-transactions (i.e. PCI)	
Safety and Wellbeing	Facilitation of the creation, transmission or sale of objectionable or pirated material (i.e. child exploitation)	Harm to individuals due to identity theft, cyber bullying or blackmail			
Disruption	Business disruption and/or impact to wellbeing due to critical infrastructure outage	Inability to facilitate secure and reliable communications channel for international relations/business	Destruction or ransom of information	Malicious altering or defacement of Government information	Interruption to logistics/travel
Trust and Reputation	Facilitation of global cyber attacks originating from the Pacific	Theft of intellectual property, personal information or sensitive data	Driving a malicious political agenda through hacktivism or social media.		

Fiji

Key Thoughts
The USA classify Fiji as "critical infrastructure and key resources abroad" due to SCCL undersea cable that is connected to FINTEL. In addition to this, Fiji's relative scale in the region (population and GDP) alongside high number of known cyber attacks (Fiji Police recorded more than 45 "major" cyber attacks over 3 years, costing locals over US$330k in stolen funds alone) drives a high relative threat profile for Fiji.

Governance of cyber security for the Fijian Government has recently shifted, and was in a transient state during our consultation mission in March 2019. Ownership of Cyber has moved from the Ministry of Defence to the Ministry of Communications. The approved National Cyber Security Strategy (~2016) was owned by the Ministry of Communications, but was not known to other officials (with the exception of the Reserve Bank).

We observed some relatively good capability for Cyber within the Fiji Police (~4 Cyber officers focused on outreach and enforcement), Reserve Bank of Fiji (~4 cyber security staff focusing on internal cyber security and compliance) and the key members of the Ministry of Communications were well briefed on cyber security for the country and region. Gaps in legislation were identified in regards to child safety and protection (The Commission of the Online Safety Act 2018 has been created to start improving in this space), and awareness of cyber security (and associated strategy/actions) was lacking outside of key people. The University of the South Pacific (USP), the major university in the region, offer two dedicated cyber security courses (a diploma and a short-course), but noted that registrations were low – both due to a lack of clear career path within Fiji, and also (anecdotally) as minimum requirements for university entrance could not be easily achieved by members of the existing workforce (i.e. Police officers).

Fijian officials cited ongoing operational funding and local staffing/ownership as the key attributes for successful cyber security initiatives in the country/region.

As high priority tasks, Fiji would benefit from:

- Establishing a CERT, which would help to provide a central point for cyber security (driving actionable information and technical support) and would also help to create a career path for USP graduates, which would help to drive local talent development.
- Clear communication and governance for cyber security. The Cyber Strategy published in 2016 was not known outside of key staff, and we could not find evidence of it in our research. While Fiji has formalised responsibility for cyber security (with Ministry of Communications), it would be valuable to communicate the Government's position and requirements through a single consistent forum.
- Improving legislation and support for Child Safety. There is an opportunity to improve the coverage of child abuse/safety cases within current legislation. The impact of the newly developed Commission of the Online Safety Act (2018) is yet to be seen as it was only recently established.

Population:
912,241 (2018; United Nations Department of Economic and Social Affairs: Population Division).

Key Economic Drivers:

- Services: 71.5%.
- Industry: 17.9%.
- Agriculture: 10.6%.
- Sugar processing makes up one-third of industrial activity.
- Travel industry.
- Tourism industry.
- Fishing industry.

Connectivity:

- International: Southern Cross Cable Network (Aus, NZ, USA).
- Local: Interchange Cable Network 1 (Vanuatu).
- Local: Tonga Cable (Tonga).
- Tui-Samoa (incomplete – Samoa, Wallis and Futuna).

Broadband Uptake:

- Fixed Line: 1.4 per 100 inhabitants (2017; ITU).
- Mobile broadband subscriptions: 55.7 per 100 inhabitants (2017; ITU).
- Mobile subscriptions 114 per 100 inhabitants (2017; ITU).
- Internet users: 46.5 per 100 inhabitants (2017; ITU).

Core Internet Uptake/Use Cases:

- Mobile banking.
- Mobile data (recreational).
- 470,000 Facebook users (51.5% penetration rate) (2017; internetworldstats).

Key Contacts:

- Minister of Communications (Secretary) – Hon. Tupoutua'h Baravilala (focal contact for cyber security).
- Minister for Communications and Public Enterprise – Hon. Aiyaz Sayed-Khaiyum (senior responsible owner for cyber security)
- Fiji Police - Serupepeli Neiko (Head of Cyber Crime Unit)
- Vice-Chancellor, University of South Pacific (USP) - Professor Pal Ahluwalia (Chair of the CROP ICT Working Group).
- Pacific Islands Forum Secretariat - Regional Security Officer (Terio Koronawa).

Key Institutions:

- Ministry of Communications (lead Ministry for cyber security)
- Fiji Police Force / Cyber Crime Unit.
- Forum Secretariat (based in Fiji)
- Reserve Bank of Fiji / Financial Intelligence Unit
- Ministry of Defence, Immigration and National Security.

Cyber Area	Current State	In-Progress / Planned

Strategy	**Strategy, Roadmap and Policy**
	• Fiji have developed and approved a national Cyber Security Strategy (~2016). The strategy is owned by the Ministry of Communications, however its existence is not well known across Government.
	• Fiji Cyber Security Working Group (est. 2011 – covering awareness, outreach, training, strategy, policy and legislation).
	
	Institutional Bodies
	• Ministry of Communications (alongside the Office of the Solicitor-General) are the lead agency for cyber security.
	• Cyber Crime Unit (est. by Fiji Police Force) have a capability which includes multiple (2-5) trained technical cyber security crime officers.
	• Commissioner of the Online Safety Act (2018) has been established to assist in promoting/regulating online safety. The Act has been critiqued for its focus on censoring social media (a regional concern).
	• Fiji Financial Intelligence Unit (investigating fraud and money laundering).
	  • Member of Pacific Islands Telecommunications Association, International Telecommunication Union and International Multilateral Partnership against Cyber Threats (ITU IMPACT), Commonwealth Telecommunications Office (CTO).
	
	Training and Awareness
	• USP has post-graduate courses available for cyber security (they noted the demand was still fairly low based on limited visibility of job opportunities after study). In some cases, candidates do not qualify for post-graduate study, and so there are barriers to entry.
	• Part of the Cyber Safety Pasifika programme for teachers and students, Fiji Police have conducted "hundreds" of awareness campaigns based on this.
	• Fiji benefitted from the "Capacity Building and ICT Policy, Regulatory and Legislative Frameworks Support for Pacific Island Countries" co-funded by ITU and the EU.
	• Interpol and FBI also offering training in cyber crime investigation.
	• IMF and SWIFT offer useful training to banks on cyber security.
	
	Risk Management
	• The Forum Secretariat (based in Fiji) completed a high-level regional risk assessment, which identified the following key risks (paraphrased):
	  1. Rapid expansion of ICT – faster than risk management.
	  2. Online scams and phishing attacks.
	  3. Card/ATM skimming by foreign nationals.
	  4. Online sexual grooming, exploitation of children and bullying.
	  5. A lack of institutional capability leading to major disruptive cyber security events.
		• The Forum Secretariat will complete cyber security maturity self-assessments against key high-level risks for the region on an ongoing basis (proposed to start this/next year).

Secure	**Legislation** The associated Chapman Tripp analysis outlines the following: • Cybercrime (substantive) – established. • Cybercrime (child protection) – none. • Cybercrime (procedural) – initial. • Electronic transactions – established. • Privacy – initial. • Data protection – initial. • Digital authentication – none. • Consumer protection – established. • Intellectual property – established. **Capability** • Fiji Police's Cyber Crime Unit includes some (2-5) trained cyber crime officers. • The Reserve Bank of Fiji employs qualified cyber security specialists (i.e. CISSP, approximately 2 dedicated staff). • Some teaching and technical capability for cyber security exists within USP (including a basic SOC capability). This technical capability is sometimes used to support the Cyber Crime Unit. • CCTLD is managed by USP on behalf of the Fijian Government. **Requirements and Standards** • None identified to date.	• A Cyber Crime Bill is currently being drafted by the Ministry of Defence, Immigration and National Security alongside consultation with the Fiji Police Force, Solicitor-General's office and all Internet Service Providers (ISPs).
Vigilant	**International Co-operation and Intel** • Member of the Pacific Island Law Officers' Network (PILON). • Member of Pacific Security Operational Network (PaCSON). • AusCERT and Australian Federal Police provides advice and support. • Fiji's USP Vice-Chancellor is the chair of the CROP ICT Working Group. **Detecting and Monitoring** • Fiji Police and the FIU keep track of cyber security incidents, of which they have responded to more than 45 major events between 2013 and 2016. Over US$330,000 was stolen from local Fijians through these attacks alone. • USP have a basic monitoring/SOC capability (for the University network only).	• None identified to date.

Resilient	**Connectivity and Redundancy** • Multiple international cables. • Comprehensive mobile broadband rollout. **Cyber Incident Response (CERT)** • (Closed) PacCERT – Cyber Emergency Response Team was located in Fiji before closing in 2014. **Cyber Crime Enforcement** • Fiji Police Force / Cyber Crime Unit (est. 2008). • Fiji Financial Intelligence Unit. • A number of cyber security crimes have been successfully detected and prosecuted in Fiji (i.e. money stolen and sent overseas and ATM skimming). • According to the Fiji Police, the Cyber Safety Pasifika programme provides a process to interact with Facebook in regards to cyber security incidents (new in 2019).	• A proposal for a "National Cyber Security Centre" (a "Fiji CERT" with some additional training/secondment opportunities) is currently before the World Bank for sponsorship. This is being led by USP. • For the 2019 financial year, a budgetary allocation has been made for a new local Fiji CERT. This is still in planning stages.
Previous Cyber Incidents	Our conversations with key stakeholder representatives identified a number of previous cyber security incidents based on anecdotal evidence: • In 2018, a fake Facebook account was created to impersonate the Fiji Times newspaper. • In 2017, some foreign nationals were arrested for using stolen bank cards to withdraw money from ATM's in Fiji. • In 2016, a fake Facebook account was created to impersonate Fiji's President, Jioji Konrote. • In 2016, a number of fake Facebook pages were created purporting to be the governance of the Reserve Bank of Fiji. These accounts were used to secure funds via deception. • There have been reports of more than US$300,000 in total theft via "fake invoicing" and spear phishing attacks (between 2013 and 2016 only). • There have been numerous reports of credit card/ATM skimming between 2003 and 2016. The largest in 2015 involved over 500 unique cards, including individual withdrawals of over US$10,000 in some cases. • 3-4 attacks have been observed that where Fiji was attributed by overseas agencies as the source. • Unlicensed telecommunications operators, i.e. facilitating international calls for profit as an unlicensed operator. The Fiji Police informed us that business/government email compromise (leading to stolen funds through fake invoicing and the release of sensitive comms) and credit card theft as the most impactful type of incidents for Fiji. It should be noted that Fiji has a much better record of past cyber security events due to having a mature Cyber Crime Unit capability (started in 2008).	

Key Cyber Risks – Fiji

Economic	Facilitation of international money laundering and funding of terrorism	Financial harm due to fraud or unauthorised access to banking	Inability to process or receive international payments	Inability to meet international standards for e-transactions (i.e. PCI)	
Safety and Wellbeing	Facilitation of the creation, transmission or sale of objectionable or pirated material (i.e. child exploitation)	Harm to individuals due to identity theft, cyber bullying or blackmail			
Disruption	Business disruption and/or impact to wellbeing due to critical infrastructure outage	Inability to facilitate secure and reliable communications channel for international relations/business	Destruction or ransom of information	Malicious altering or defacement of Government information	Interruption to logistics/travel
Trust and Reputation	Facilitation of global cyber attacks originating from the Pacific	Theft of intellectual property, personal information or sensitive data	Driving a malicious political agenda through hacktivism or social media.		

Kiribati 

Key Thoughts
Kiribati has a low maturity across cyber security, especially considering its relative size in the region. While the telecommunications market is open for competition, there is currently no submarine cable (satellite only) and two ISPs operating in the space.

Kiribati's risk landscape is rapidly increasing with the uptake of Visa payment cards (power and water bills can both be paid online), the NEXT submarine cable (due to be completed by the end of 2019), and the ongoing move to online banking (currently for balances but not payments). There was also a concern in regards to the use, transfer and/or creation of child pornography in Kiribati – which is also reflected by the amendments to the Communications Act in late 2016 – which broaden the scope of this Act in regards to child pornography.

Representatives from Kiribati informed us that their culture is very open, and as such there was no demand for privacy laws – which is aligned with a number of other Pacific Island countries we examined.

As high priority tasks, Kiribati would benefit from:
- Confirming that cyber security ownership is with an entity that can provide adequate coverage for Government and critical infrastructure, and developing an action plan that aligns with their overarching strategies for ICT and development.
- Building additional investigation and enforcement capability in regards to child protection, to support the additions to the Communications Act.
- Establishing or building a formal relationship with a CERT, to provide technical expertise and support in the case of a major cyber security incident.

Population:
118,414 (2018; United Nations Department of Economic and Social Affairs: Population Division).

Key Economic Drivers:
- Natural resources (such as copra, coconuts, breadfruit, and fish).
- Fishing licences
- International remittance
- Tourism.
- Development assistance & foreign aid.

Connectivity:
- No submarine cable (NEXT cable planned for end of 2019).
- International: Satellite Uplink.
- Local: 4G and 3G mobile coverage.

Broadband Uptake:
- Fixed Line: 1.1 per 100 inhabitants (2017; ITU).
- Mobile: 42 per 100 inhabitants (2017; ITU).
- Internet users: 13.7 per 100 inhabitants (2017; ITU).

Core Internet Uptake/Use Cases:
- Mobile data (recreational).
- 10,000 Facebook subscribers (8.6% penetration rate) (2017; internetworldstats).
- 39.6 Mobile/cellular subscribers per 100 inhabitants (2017; ITU).

Key Contacts:
- Minister for Communications, Transport and Tourism Development – Hon. Willie Tokataake.
- Director of ICT – Wayne Reiher.
- Attorney General – Tetiro Semilota.

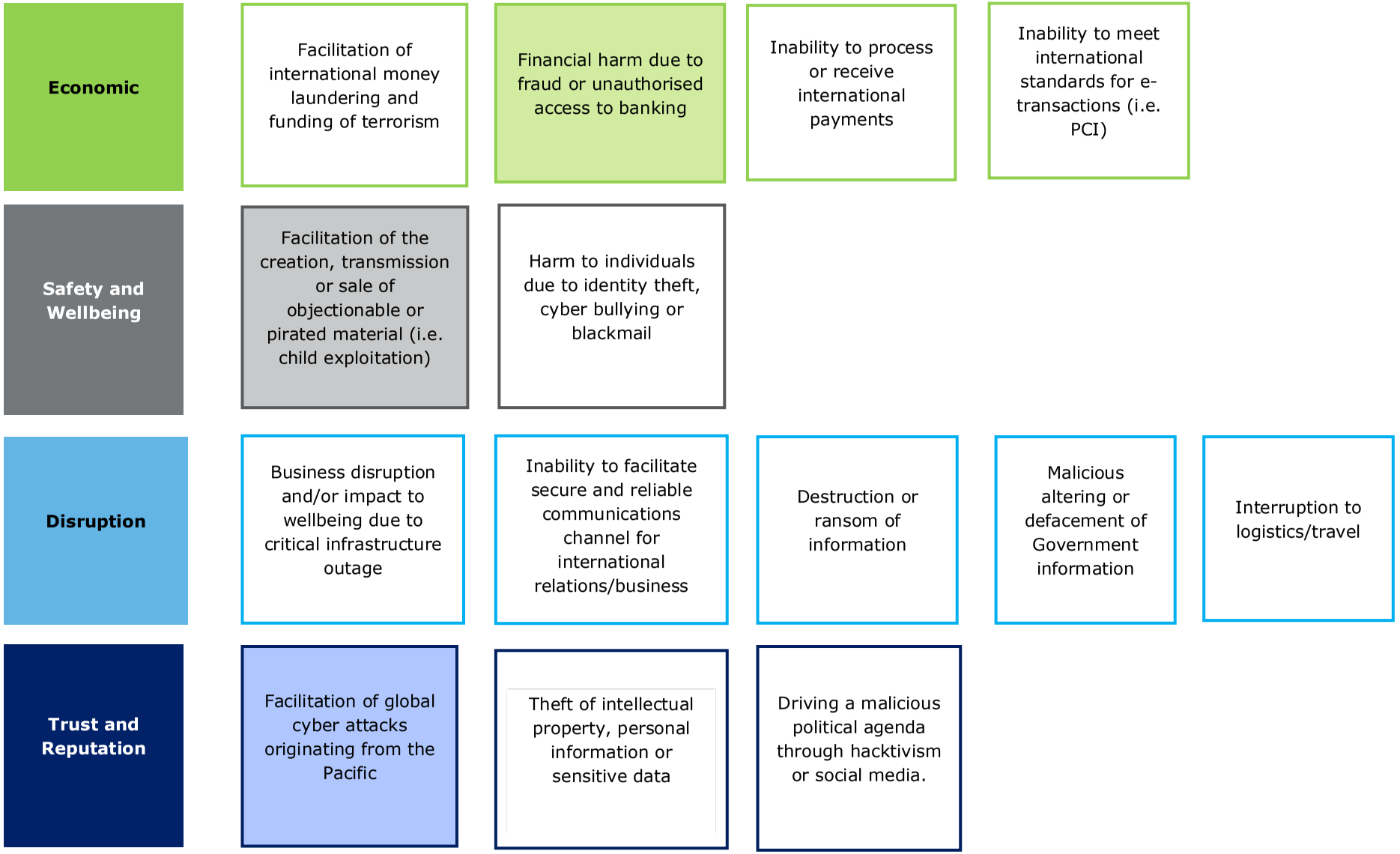
Key Institutions:
- Kiribati Police Service (including the Financial Intelligence Unit).
- Communications Commission of Kiribati (CCK) – governing authority of information, communications and technology. Established to implement and enforce the provisions of the Communications Act 2013.
- Ministry of Information, Communication, Transport and Tourism (MICTTD) – responsible for ICT.
- ICT Working Group (chaired by the Director of ICT).

Cyber Area	Current State	In-Progress / Planned

Strategy	**Strategy, Roadmap and Policy** • No dedicated cyber security strategy has been identified. • National ICT Policy (2011; MCTTD) – which mentions cyber security, but is outdated. • The "Telecommunications and ICT Development" project has four components: ICT policy and legal support; ICT regulatory support; outer islands connectivity; and project management (2013; CommonWealthOfNations). **Institutional Bodies** • Communications Commission of Kiribati (CCK) is the regulator for the Telco sector, and has overall responsibility for cyber security. • Ministry of Communications, Transport and Tourism Development (MCTTD) is responsible for ICT. • Policy Administration and Support Services Division – undertakes the admin support and advice for MCTTD. • ICT Policy and Development Division – provides ICT support to MCTTD. • ICT Working Group was established in 2016 – which includes some cyber security elements. **Training and Awareness** • CCK runs IT courses. • CCK has completed radio-based messaging to help parents and their children remain safe online. **Risk Management** • None identified to date.	• The ICT unit in the Ministry for Communications, Transport and Tourism Development is officially recognised agency for implementing a national cyber security strategy, policy and roadmap. • Kiribati Development plan 2016 – 2019 highlights a want for an increased rate of usage for mobile phones and Internet (2016; MCTTD). • MICTTD Strategic Plan 2016-2019. • Develop cyber security – funding required.
Secure	**Legislation** The associated Chapman Tripp analysis outlines the following: • Cybercrime (substantive) – established. • Cybercrime (child protection) – established. • Cybercrime (procedural) – established. • Electronic transactions – none. • Privacy – initial. • Data protection – none. • Digital authentication – none. • Consumer protection – established. • Intellectual property – initial. **Capability** • None identified to date. **Requirements and Standards** • None identified to date.	• MICTTD Strategic Plan 2016-2019 - Improve a strong and functioning legal framework - Review and amend Communications Act 2016 - Security Policy and Legislation - $500,000 budget.

Vigilant	**International Co-operation and Intel** • Member of Pacific Islands Telecommunications Association, ITU IMPACT, Commonwealth Telecommunications Office (CTO), South Pacific Community (SPC), World Bank (WB), Asia Pacific Telecommunity (APT), Pacific Islands Telecommunication Association (PITA). • Extradition Act 2003 covers offences with a minimum 1 year imprisonment, which may include cyber security offences. • Mutual Assistance in Criminal Matters Act 2003 contains reasonably extensive provisions, including search and seizure powers and evidence protection, which likely covers cyber security related issues. • Member of the Pacific Island Law Officers' Network (PILON). • Member of Pacific Cyber Security Operational Network (PaCSON). **Detection and Monitoring** • None identified to date.	• None identified to date.
Resilient	**Connectivity and Redundancy** • The market has recently been opened for multiple ISPs, which are: - Amalgamated Telecom Holdings Kiribati Limited (ATHKL). - Ocean Link (a China-based mobile company that has recently opened) • Local 3G and 4G mobile infrastructure is provided by ATHKL. • 5 Satellites providing international bandwidth. **Cyber Incident Response (CERT)** • Kiribati has no CERT (before it closed, Kiribati was a member of PacCERT/PacINET). **Cyber Crime Enforcement** • The PILON respondents from Kiribati noted that they would look to the New Zealand and Australian Federal Police for assistance in investigating cyber crime. • Financial Intelligence Unit has been established within the Kiribati Police Force to investigate money laundering and financial crime.	• Signed contract for 'NEXT submarine cable', going live end of 2019 (2018; ZDNet). • A backup communication system for disaster recovery is part of the Strategic Plan 2016-2019.
Previous Cyber Incidents	Based on our conversations with key stakeholder representatives, we have captured a number of previous cyber incidents based on anecdotal evidence: • The Kiribati Government was defrauded by an attacker who had gained access to a Government email account. • The Kiribati Government are working with the UK Police to apprehend and prosecute a suspect of cyber crime located in the UK. • There was a concern about use, creation and/or transmission of child pornography. • There have been reports of online scams – typically emails which trick users into sending money abroad.	

Key Cyber Risks – Kiribati



Republic of the Marshall Islands 

Key Thoughts

The Republic of the Marshall Islands (RMI) has close ties with the United States of America (USA) due to its location, history with the US, and the US military base which operates on one of the islands. This relationship is reflected in national identity cards (including Social Security Numbers (SSNs)), constitutional provisions for privacy (and an increased public desire for privacy as compared to other island nations), and access to support from the Federal Bureau of Investigation (FBI) for cyber security. The Constitution of the RMI includes some provisions for privacy, which is unlike other Pacific Islands, however these provisions are not currently supported by legislation.

Contextually, there is very low credit/debit card penetration in the RMI. During our visit in early 2019, there were only three ATMs on Majuro and the majority of local stores only accepted cash. There is only one Telco/ISP, Marshall Islands National Telecommunications Authority (NTA) – driving relatively high prices for connectivity and limited international roaming capability for visitors. While domestic/internal bandwidth is limited and expensive, significant international capacity is available (80Gbps available, only 4Gbps currently in use). Based on our consultations, we identified the following systems/services as having relatively high cyber security risk in RMI:

- The social security system – similar to the system used in the USA, each citizen has a unique social security number. The data for this system is stored on Majuro only (in 2 places), creating a physical disaster risk which could result in a total loss of this information. The system is administered by the Marshall Islands Social Security Administration (MISSA).
- The electricity industrial control system – Marshalls Energy Company has recently implemented a digital control system (industrial control system) to control the power grid within Majuro. This system will be expanded by the pending ~US$30m solar project funded by the World Bank.
- The shipping registry – is a large data set tracking vessels which are registered to the RMI. These system has already had some cyber security assessment and utilises additional controls to most other systems in RMI.
- The RMI Police database – while RMI Police are largely using paper-based systems, they have a central database of information which is a Microsoft Access database. It is likely that this database contains sensitive information, and typically older Microsoft Access databases are challenging to adequately secure.

A lack of training and documentation for existing systems means that several key Government systems in RMI are currently not operational.

The Ministry of Transport, Communication and Information Technology ('TCIT', previously the Ministry of Transport and Communication) has been established as the lead agency for ICT and cyber security, since circa early 2019. Each Government ministry currently has its own ICT team/capability. This approach creates challenges based on procuring and maintaining separate technology, and based on the low availability of skilled ICT staff (and teachers) to support multiple teams. The maturity level of cyber security across Government is low, however there are pockets of capability – including a digital forensics specialist within the Auditor-General's Office. A number of Government ministries use Google Gmail or similar for email. Recently, the Ministry of Finance has moved to a private domain for email, based on previous large phishing and fraud attempts.

As high priority tasks, the Republic of the Marshall Islands would benefit from:

- Developing a cyber security strategy and approach/action plan that is clearly owned and driven by Government, alongside confirming this forms part of the National Strategic Plan.
- Baseline security awareness training to Government and critical infrastructure staff, especially for senior staff and those who are involved in finance/payments. A briefing pack including baseline knowledge, local context and regional activity was suggested.
- Building the capability of and further formalising institutional leadership/roles for cyber security within TNC.
- Completing the eGovernment project / capability development, confirming it includes security and relevant training in its design and budget (i.e. security architecture, testing, training, and ongoing maintenance and monitoring).
- Assess and mitigate security risks created by the National Cryptocurrency and World Bank solar power (and control system) projects (based on our interviews, cyber security has not been considered as a part of these projects).

Population:
53,167 (2018; United Nations Department of Economic and Social Affairs: Population Division).

Key Economic Drivers:
- Shipping.
- Agriculture.
- Coconut and copra.
- Handcrafts.
- Sale of fishing rights.
- Tourism.
- Foreign aid from United States – now discontinued (MI GDP is $115 million, US aid to MI is $30 million).

Connectivity:
- International: Single cable (HANTRU1 Cable System to Majuro and Kwajalein).
- International: Telephone satellite communication (Intelsat).
- Local: Shortwave radiotelephone where no connection between islands.
- US military base on Kwajalein has its own satellite communication system.
- National Telecommunications Authority (NTA) is the sole provider for domestic and international voice, fax, data, and Internet services.

Broadband Uptake:
- Fixed Line: 2.6 per 100 inhabitants (2017; ITU).
- Mobile: 0 per 100 inhabitants (2017; ITU).
- Internet users: 29.8 per 100 inhabitants (2017; ITU).

Core Internet Uptake/Use Cases:
- Mobile data (recreational).
- Social media.
- 21,000 Facebook users (19.9% penetration rate) (2017; internetworldstats).

Key Contacts:
- Minister for Transportation, Communication and Information Technology (TCIT) – Hon. Phil Philippo (focal point for Cyber).
- Head of Cyber Unit, RMI Police – Mr. Verny Wase
- Acting Attorney General – Mr. Jonathan Kawami

Key Institutions:
- Ministry of Transport, Communication and Information Technology.
- National Telecommunications Authority (NTA).
- Attorney General's Office.

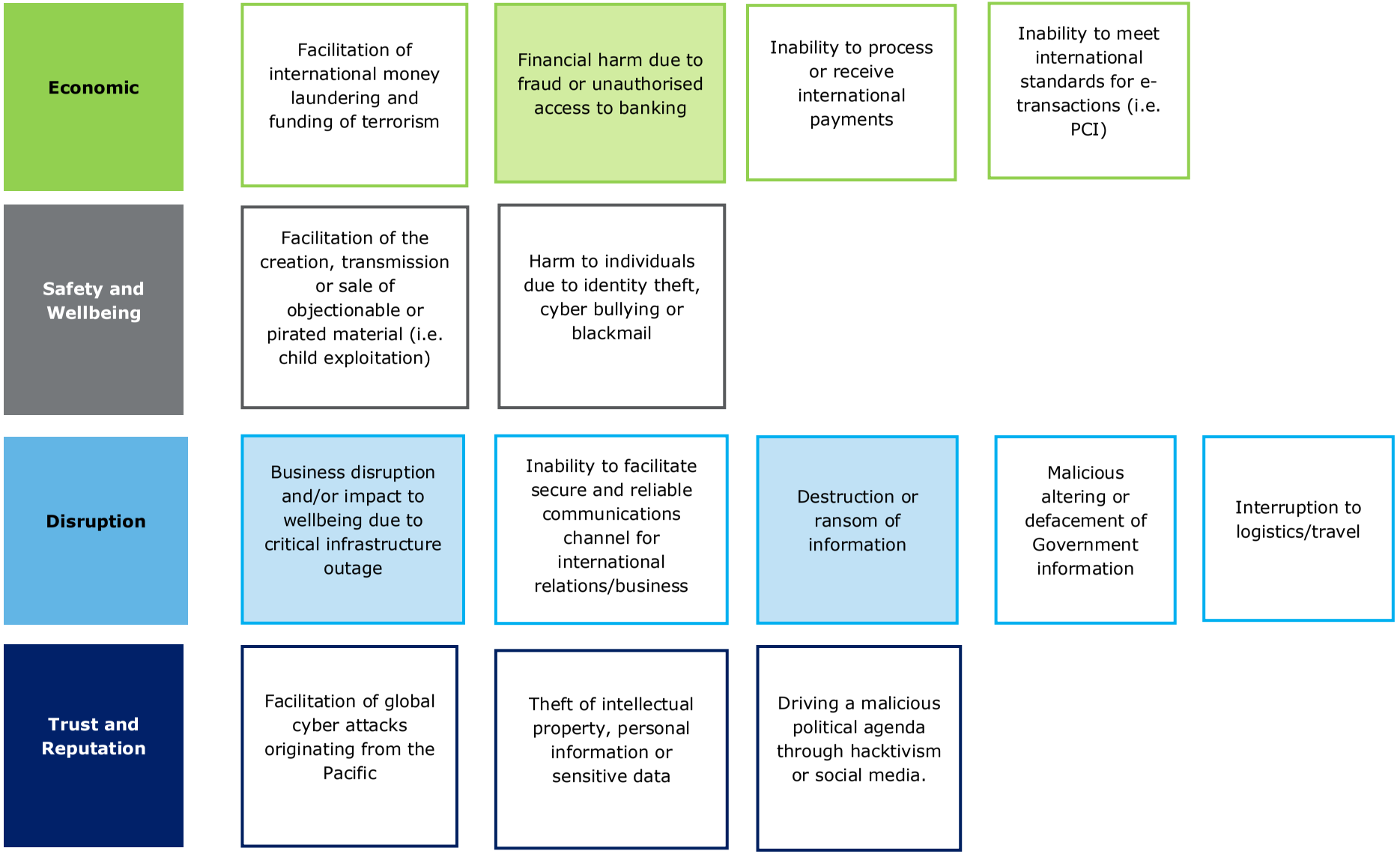
Cyber Area	Current State	In-Progress / Planned

Strategy	**Strategy, Roadmap and Policy** • No overarching cyber security strategy. **Institutional Bodies** • The Ministry of Transport and Communication, which now includes information technology and are the focal point for cyber security (since circa early 2019). • The National Telecommunications Authority (NTA) is a public-private organisation responsible for ICT support and are key contact point for technical cyber security assistance. • The RMI Police have a Cyber Unit, led by Mr. Verny Wase. • The RMI Information Security Governance Taskforce was established in 2017. There remit is to assess current state, establish policy, modernise, and improve storage and sharing of information within Government. • The Auditor-General have a digital forensics specialist. **Training and Awareness** • Taking part in the Cyber Safety Pasifika Programme (cyber training for teachers and students). • ICT and cyber security training is available from the University of South Pacific campus based in the Republic of the Marshall Islands, however uptake has been low. • APNIC and PITA provide training to NTA, which includes cyber security. **Risk Management** • None identified to date.	• The Republic of the Marshall Islands announced a plan in February 2018 to issue its own cryptocurrency, called 'The Sovereign'. It is being built by an Israeli start-up called Neema. • RMI are currently working with the World Bank on an eGovernment project to centralise their ICT infrastructure/capability (lead by James Newman at World Bank).
Secure	**Legislation** The associated Chapman Tripp analysis outlines the following: • Cybercrime (substantive) – initial. • Cybercrime (child protection) – initial. • Cybercrime (procedural) – initial. • Electronic transactions – none. • Privacy – established. • Data protection – initial. • Digital authentication – initial. • Consumer protection – established. • Intellectual property – initial. **Capability** • There is a local resource who has completed training in digital forensics (currently based in the Auditor's Office). **Requirements and Standards** • There are not currently any requirements or standards, and the Office of the Auditor-General does not currently perform IT security auditing for Government.	• There has been work towards drafting a Computer Crimes Bill for RMI, started in 2011. This was originally based on the Tongan Computer Crimes Act 2003. This work is currently on hold. • The Marshalls Energy Company (MEC) is moving to solar technology, and working with the World Bank on a ~US$30m project to add an additional 4.5MW of solar power. These systems will include industrial control systems (ICS) which are used to control the power. These systems are prone to attack and should be appropriately secured.

Vigilant	**International Co-operation and Intel** • Federal Bureau of Investigation (FBI) in Guam. • Pacific Islands Law Officer's Network (PILON). • Pacific Cyber Security Operational Network (PaCSON) – which interviewees noted was useful but they hope to receive more hands-on training. • Pacific Islands Telecommunications Association. • ITU IMPACT. • Commonwealth Telecommunications Office (CTO). • APNIC. **Detection and Monitoring** • NTA stores phone and text messages records, which can be provided for an investigation based on a court order.	• None identified to date.
Resilient	**Connectivity and Redundancy** • HANTRU1 submarine cables (two cables) provide adequate international capacity. • Mobile broadband is available on the main islands – but domestic connectivity is constrained. • A number of Government servers have additional backups, but mostly they are based locally. • The National Telecommunications Authority (NTA) partners with ICANN to host the L-Root Server Instance. ICANN, the global body that manages addresses online, manage 13 root servers to give the Domain Name System (DNS) resiliency, A through to M. DNS is one of the backbones of the Internet. **Cyber Incident Response (CERT)** • No CERT (The Republic of the Marshall Islands was a member of the now closed PacCERT). **Cyber Crime Enforcement** • None identified to date.	• RMI Police have been considering the possibility of a local CERT, which would include: Police, Auditor-General, Attorney-General, NTA, and the Ministry of Transportation, Communication and Information Technology.

Previous Cyber Incidents	Based on our conversations with stakeholder representatives, we have captured a number of previous cyber security incidents based on anecdotal evidence: • In early 2018, there were successful attempts to hack into Government accounts and extract large sums of money. Although the money was successfully extracted, this activity was quickly flagged and investigated with assistance from the Australian Federal Police and a local resource. The FBI in Guam were able to assist. Funds were recovered in full. • There have been a large number of other targeted email phishing attacks focused on extracting money. These have been specifically targeted at senior people within major organisations. • Fake social media pages purporting to be a number of different Government officials and prominent figures in the Marshall Islands. • Cyber bullying, including some serious cases where offensive material has been created. There were ongoing cases at the time of our consultation. Generally, however, we were told by multiple interviewees that cyber bullying was less prevalent than in some other countries in the region for cultural reasons. • Two significant distributed denial of service attacks have impacted connectivity for RMI, but not recently. • NTA has previously suffered a Ransomware attack, but were able to recover from backups. • Card skimmers have been identified on ATMs. • Fraud and scam events affecting citizens have been reported, especially people imitating the local businesses and Government agencies.

Key Cyber Risks – Republic of the Marshall Islands



Nauru 

Key Thoughts
Nauru is a relatively small Pacific Island nation, with a population just over 11,000 (2018). They do not currently have a submarine cable for high speed internet, although ADB and the World Bank have committed (May 2018) to building a submarine cable to assist Nauru.

Based on our desk-based research (Nauru's representatives were reluctant to engage us at PILON), Nauru are relatively immature in their overarching approach to cyber security and ICT. This is evidenced by the lack of strategy and clarity in regards to institutional leadership. The Nauru Government ICT Department website was unavailable during our research period.

We found evidence that a Cyber Safety Task Force was established in Nauru previously, and that the Nauru Police Force have provided some cyber security awareness and outreach for the community as a part of the Cyber Safety Pasifika programme.

Facebook was banned by the Nauru Government in 2015, on the basis of targeting "criminals and sexual perverts" using the platform. Some public opinion was that the Facebook ban was executed to reduce criticism of Government and control the flow of information. Based on public push-back, the Facebook ban was lifted in 2018.

Population:
11,312 (2018; United Nations Department of Economic and Social Affairs: Population Division)

Key Economic Drivers:
- Phosphate mining (as of 2000 not economically viable, continues at small scale).
- Offshore banking, Nauru was a tax haven up to 2003.
- Australian detention facilities.
- Foreign aid. Nauru's GDP is roughly $150 million, Australia's foreign aid is roughly $25 million (excluding employment from detention centres).

Connectivity:
- No submarine cable.
- International: Telephone systems provided by Australian facilities (local/international).
- Local: Copper wire, fibre and radio.

Broadband Uptake:
- Fixed Line: 0 per 100 inhabitants in 2016 (2017; ITU).
- Mobile: 32.6 per 100 inhabitants in 2016 (2017; ITU).
- Internet users: 54% of the population in 2016 (2017; ITU).

Core Internet Uptake/Use Cases:
- Mobile data (recreational).
- 3,400 Facebook users (29.9% penetration rate) (2017; internetworldstats).

Key Contacts:
- Minister for Transport and Communication – Hon. Shadlog Bernicke.
- Attorney General – Baron Waqa.

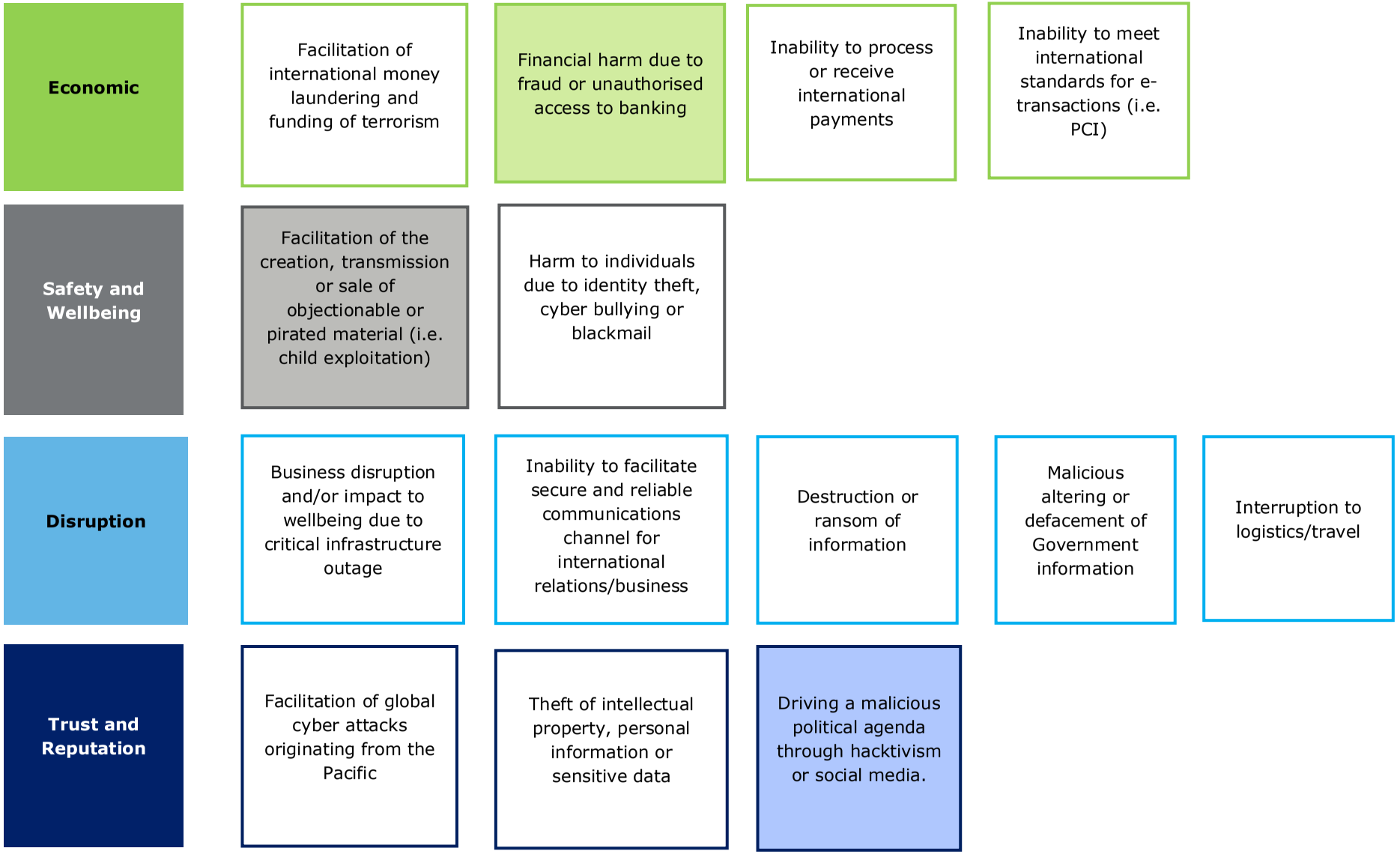
Key Institutions:
- Cyber Safety Task Force.
- Government ICT Department.
- Nauru Police Force (part of Cyber Safety Pasifika).
- Australian High Court (legal matters can be taken to Australia if people seek a higher court of adjudication.
  RONTel (Republic of Nauru Telecommunications Corporation).
- CenpacNet Inc (ISP and provide ccTLD services).

Cyber Area	Current State	In-Progress / Planned

Strategy	**Strategy, Roadmap and Policy** • No overarching cyber security strategy. **Institutional Bodies** • Ministry of Transport and Communication. • Government ICT Department (provide ICT support to local Government). • CenpacNet Inc. (jointly owned and operated by RONTel and the Ministry for Nauru Phosphate Royalties Trust) provide ccTLD services. **Training and Awareness** • The Nauru Police Force are taking part in the Cyber Safe Pasifika Programme (cyber security training for teachers and students). **Risk Management** • None identified to date.	• The Minister of Telecommunications has an initiative to install 4G mobile data technology across the country.
Secure	**Legislation** The associated Chapman Tripp analysis outlines the following: • Cybercrime (substantive) – sophisticated. • Cybercrime (child protection) – sophisticated. • Cybercrime (procedural) – sophisticated. • Electronic transactions – none. • Privacy – initial. • Data protection – none. • Digital authentication – none. • Consumer protection – initial. • Intellectual property – initial. **Capability** • None identified to date. **Requirements and Standards** • None identified to date.	• None identified to date.
Vigilant	**International Co-operation and Intel** • Member of Pacific Islands Telecommunications Association, ITU IMPACT, Commonwealth Telecommunications Office (CTO). • Member of the Pacific Island Law Officers Network (PILON). **Detection and Monitoring** • None identified to date.	• None identified to date.

Resilient	**Connectivity and Redundancy** • Multiple ISPs (CenpacNet and Digicel Nauru). **Cyber Incident Response (CERT)** • No CERT. • Nauru was a member of PacCERT (now closed). • Nauru is a member of the Pacific Region Cybercrime Criminal Justice Network. **Cyber Crime Enforcement** • The agency responsible for cyber security is the Cyber Safety Task Force. A joint force compromising of members from the Government ICT Department, the Justice and Border Control, and the Police Force. • Cyber crime prosecutions are handled by the Office of the DPP.	• In May 2018, ADB and World Bank announced co-financing for a project building a submarine cable to provide broadband in Nauru (and Kitibati).
Previous Cyber Incidents	Nauru's Government implemented blocking of Facebook from 2015 to 2018 (when they decided to lift the ban). The reasoning for the ban was to target "criminals and sexual perverts"). We have not identified any other previous cyber security incidents based on desk-based research.	

Key Cyber Risks – Nauru



Niue 

Key Thoughts
Niue is unique in that the population is only circa 1,600. This drives a need for shared institutional/role responsibility and international support for cyber security. While connectivity is still relatively limited (a submarine cable is due to be completed in 2020) using satellite, the penetration of internet use and digital payments is relatively high comparative to the region. This may be due to a close relationship with New Zealand, including the presence of Kiwibank and associated VISA and online banking capabilities. In addition, Niue provides state-funded internet to all inhabitants and a laptop to every child in school – which drives higher computer literacy and internet uptake.

Niue are a part of Cyber Safety Pasifika, although the officer who was trained in cyber security awareness has since left the police. The NZ Parliamentary Council Office (PCO) provided support in drafting cyber crime legislation, but this has not yet been passed into law. Representatives from Niue informed us that privacy is not a major concern for most inhabitants, which is aligned with the expectations of a country this size. There is no current privacy law or requirements. In the past, Niue have formed a cross-agency team to assist in cyber incident response, and also look to the NZ Police for cyber investigation support (informally).

Generally, representatives from Niue suggested that building awareness of cyber security risk and basic cyber security hygiene would be the most important activity related to cyber security.

As high priority tasks, Niue would benefit from:
- Cyber security awareness, outreach and basic training for schools, communities and Government.
- Formalised cyber incident response and investigation support (Niue is likely too small to support its own CERT).
- Cyber crime legislation and associated enforcement training for police, lawyers and judiciary.

Population:
1,624 (2018; United Nations Department of Economic and Social Affairs: Population Division).

Key Economic Drivers:
- Foreign Aid (New Zealand).
- Trade.
- Mining.
- International remittances (formerly).

Connectivity:
- International: No submarine cable – connectivity is via O3B satellite.
- International: State-owned Telecom Niue is the only commercial provider of fixed line, mobile, and ADSL services.
- International: The other telecom company in Niue is the Internet Users Society Niue (IUSN), trading as Internet Niue, which provides free Wi-Fi internet access to the whole island.
- **Local:** Mobile GSM services became available in 2011.

Broadband Uptake:
- Fixed Line: 1,224 (2003, Wikipedia).
- Mobile: 23,700 (2003, Wikipedia).
- Internet users: 1,100 as of March 2017 (internetworldstats).

Core Internet Uptake/Use Cases:
- Online banking.
- 700 Facebook users (43.4% penetration rate (2016; internetworldstats).

Key Contacts:
- Minister of Police and National Security.
- Minister of Post and Telecommunications.
- Minister of Justice, Lands and Survey.

Key Institutions:
- Ministry of Justice (potential lead for cyber security).
- Niue Police.
- Information Technology Services of Telecom Niue.
- Rocket Systems (IUSN).
- Internet Users Society-Niue (IUS-N) (NFP that funds low cost or free internet services for Niue, in practice offers free internet to government and citizens).

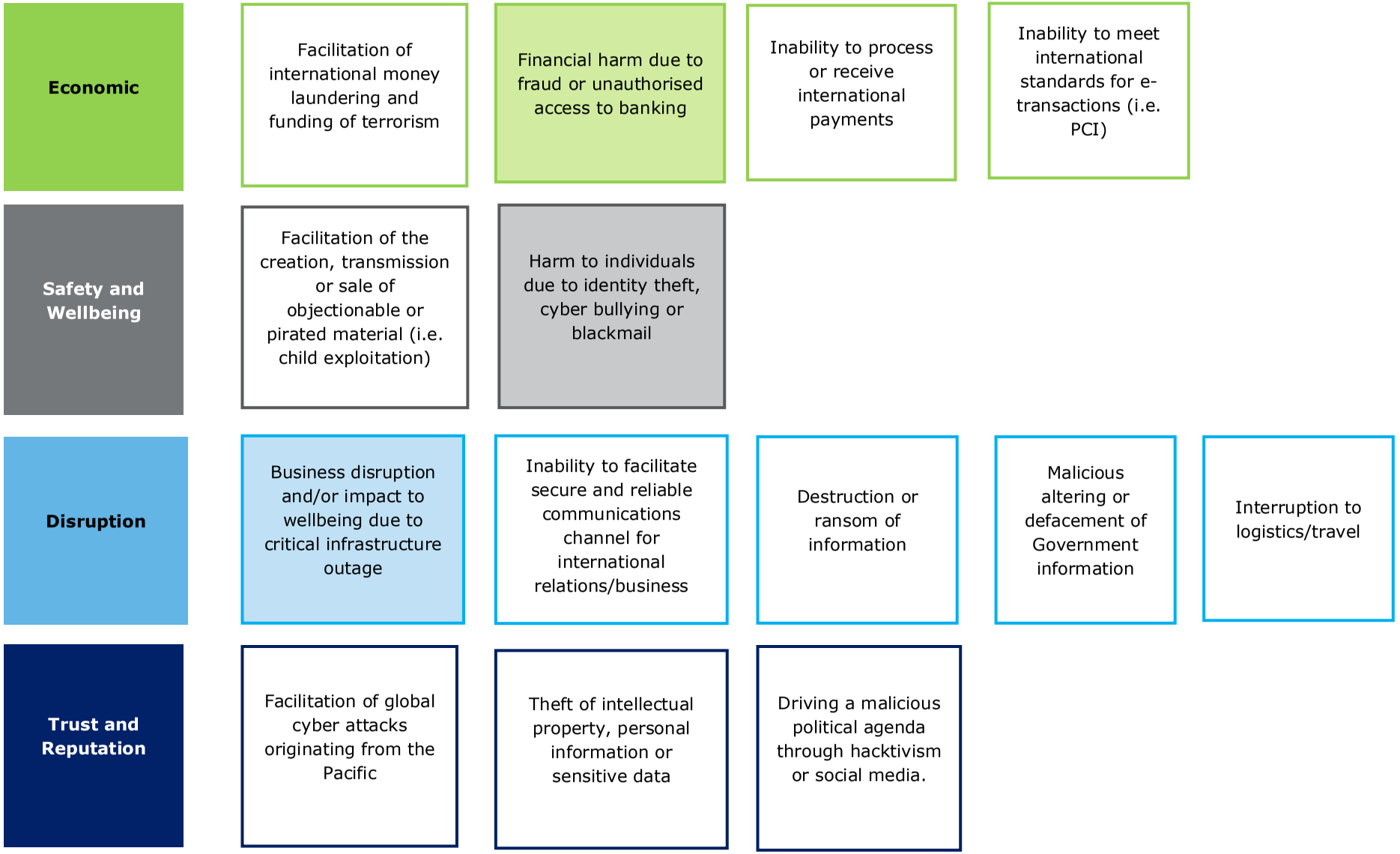
Cyber Area	Current State	In-Progress / Planned
Strategy	**Strategy, Roadmap and Policy** • No overarching cyber security strategy. • The Niue Integrated Strategic Plan (NISP) lists as part of its infrastructure plan that the Government will explore and encourage Information Communication Technology (ICT). **Institutional Bodies** • Niue has formed a cross-agency incident response team. • Ministry of Justice is the informal lead for cyber security. • Government IT department provides some technical support. **Training and Awareness** • A police officer was providing cyber security awareness and outreach as a part of Cyber Safety Pasifika (but has now left the police). • Laptops are provided to all school students to increase ICT engagement. **Risk Management** • None identified to date.	• None identified to date.
Secure	**Legislation** The associated Chapman Tripp analysis outlines the following: • Cybercrime (substantive) - established • Cybercrime (child protection) – none. • Cybercrime (procedural) – initial. • Electronic transactions – established. • Privacy – initial. • Data protection – initial. • Digital authentication – none. • Consumer protection – established. • Intellectual property – established. **Capability** • No cyber specific capability identified to date. **Requirements and Standards** • None identified to date.	• Cybercrime bill drafted in 2016 but has not been adopted. Drafting was supported by the NZ Parliamentary Council Office.

Vigilant	**International Co-operation and Intel** • The Internet Users Society, Niue (ICANN ALS) is also involved in international cyber security cooperation, and includes Information Technology Services of Telecom Niue and Rocket Systems. • Niue is a member of the Pacific Internet Society (PICSOC), PacINET and the Pacific ICT Regulatory Development Project. • Niue is a part of a joint initiative of the Australian Department of Broadband, Communications and the Digital Economy (DBCDE) and the Australian Aid Agency (AusAID) to implement anti-spam legislation in Pacific nations. • Member of the Pacific Island Law Officers Network (PILON). • Member of Pacific Cyber Security Operational Network (PaCSON). • New Zealand Police provide some informal cyber investigation support. **Detection and Monitoring** • Facebook has been blocked in schools. • The Trans-National Crimes Unit (TCU) sends information to the main TCU hub in Samoa.	• None identified to date.

Resilient	**Connectivity and Redundancy**
	• First country in the world to provide wireless internet to all inhabitants (through IUS-N).
	• Provides phone landlines to all inhabitants.
	• Laptops (OPC XO-1) are provided to all school students through the 'One Laptop per Child' project.
	• IUS-N provides government with a "secure DSL connection" to IUS-N's satellite Internet link.
	• Internet is provided for free by IUS-N to government departments and private citizens.
	• Multiple ISPs:
	  ○ Telecom Niue
	  ○ Lemko.
	
	Cyber Incident Response (CERT)
	• No CERT.
	
	Cyber Crime Enforcement
	• Niue Transnational Crimes Unit (TCU).
	• The Niue Police Department, the Information Technology Services of Telecom Niue and Rocket Systems (IUSN) form a joint response team in the event of a cyber security breach.
		• Niue will be connected to the Manatua submarine broadband cable, which is due to be completed in May 2020.
		• Telecom Niue is installing a fibre-optic cable around the island to provide a multimedia system capable of carrying voice, data, and TV services to every village in Niue.

Previous Cyber Incidents	Based on our conversations with stakeholder representatives, we have captured a number of previous cyber security incidents based on anecdotal evidence: • There have been a number of private and Government entities that have been impacted by ransomware – which encrypts/locks data and asks for a ransom to release it.	

Key Cyber Risks – Niue



Palau 

Key Thoughts
Palau is a North Pacific nation that is aligned with the United States. They have had a submarine cable for broadband connectivity since 2017, which representatives told us drove a major shift in culture and interest in regards to online services. Representatives also noted that credit card penetration was relatively high.

Based on our research, cyber security in Palau is immature. There is no current strategy or clear institutional leadership, no cyber security crime legislation, and training and awareness is limited. In addition, there is very little local investigation or response capability.

As high priority tasks, Palau would benefit from:
- Formalise institutional ownership of cyber security, and establish an overarching strategy and work plan for uplifting capability.
- Re-engage the local police with the Cyber Safety Pasifika programme, to re-train and provide awareness and outreach activities for communities.
- Formalise cyber incident response support / relationships.

Population:
21,964 (2018; United Nations Department of Economic and Social Affairs: Population Division).

Key Economic Drivers:
- GDP – US$300m (2017; Budde)
- Tourism.
- Subsistence agriculture.
- Fishing.
- Exports (fish and garments)
- Financial aid (US$800m between 1994-2009).

Connectivity:
- International: Fibre-optic submarine cable.
- Local: Satellite uplink.

Broadband Uptake:
- Fixed: 1,224 users – 5.7% (2015; BuddeComm).
- Mobile: 23,700 users –111% (2015; BuddeComm).
- 7,700 Internet users (35.4% penetration) (2017; internetworldstats).

Core Internet Uptake/Use Cases:
- Recreational.
- 6,400 Facebook users in 2016 (29.5% penetration rate) (2017; internetworldstats).

Key Contacts:
- Minister of Public Infrastructure, Industries and Commerce – Hon. Charles Obichang.
- Chief of Communications – Jonathan Temol.
- Mr. Richard Misech, CEO Palau National Communications Corporation (PNCC) and Chairman of the PITA Disaster Management Working Committee (as of 2011).

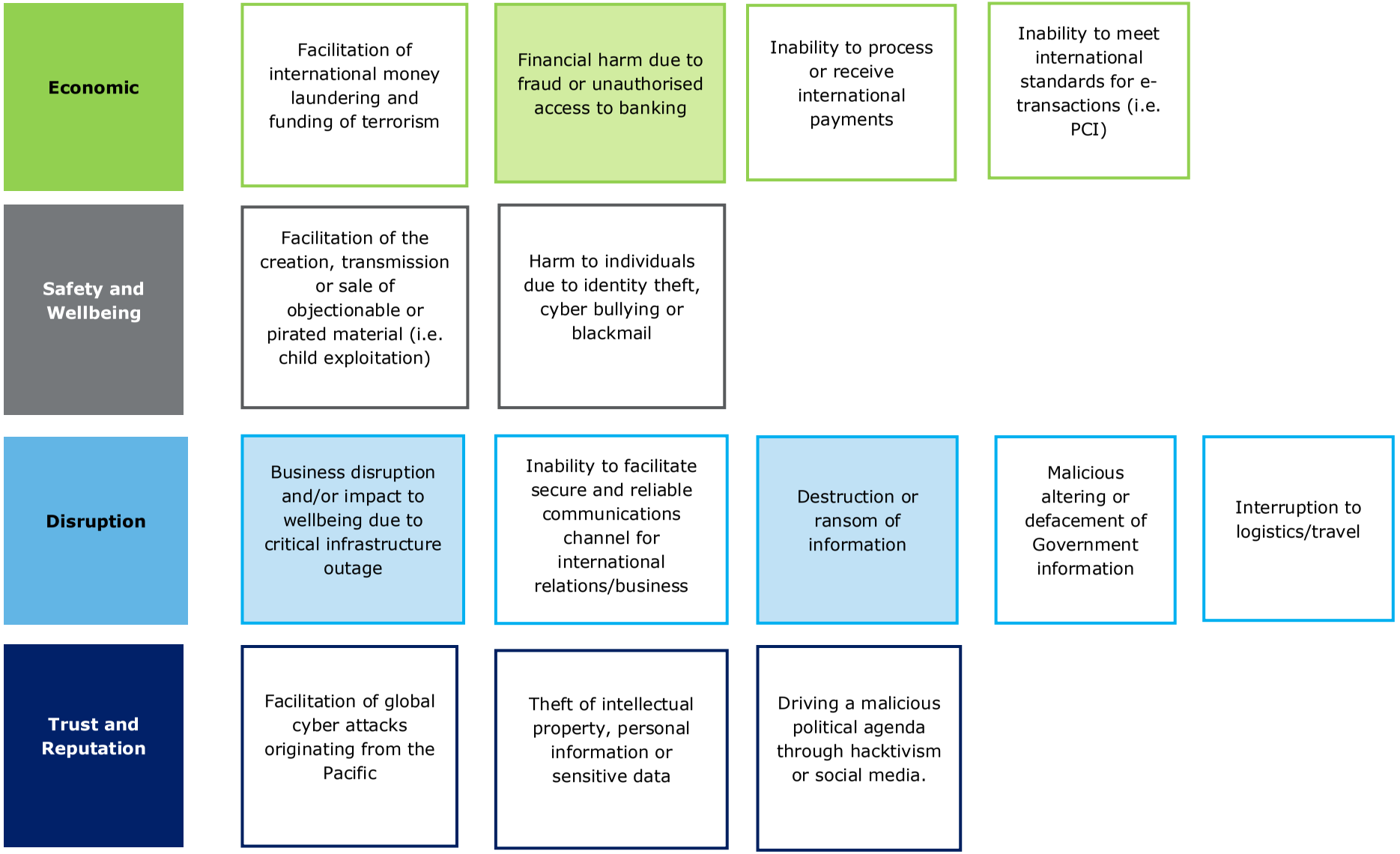
Key Institutions:
- Ministry of Public Infrastructure, Industries and Commerce.
- Palau National Police Force.
- PalauNet (formerly the Palau National Communications Corporation).
- Palau Telecom.
- Bureau of Communications (proposed in Dec 2017).

Cyber Area	Current State	In-Progress / Planned

Strategy	**Strategy, Roadmap and Policy** • No overarching cyber security strategy. • Palau National Telecommunications Act 2017 is in place to provide market regulation and continuity of service, though it appears no regulator exists yet. **Institutional Bodies** • Ministry of Public Infrastructure, Industries and Commerce. • PalauNET / Palau National Communication Corporation (PNCC) – provide telecommunication services and some ICT support. **Training and Awareness** • Training for one Police Officer provided by Australia. **Risk Management** • None identified.	• The World Bank is supporting the Palau Government in implementing ICT reform alongside the Palau-Federated States of Micronesia connectivity project, which will provide funding for telecom infrastructure.
Secure	**Legislation** The associated Chapman Tripp analysis outlines the following: • Cybercrime (substantive) – initial. • Cybercrime (child protection) – established. • Cybercrime (procedural) – initial. • Electronic transactions – none. • Privacy – initial. • Data protection – initial. • Digital authentication – none. • Consumer protection – established. • Intellectual property – established. **Capability** • One Police Officer has received some cyber security training provided by Australia. • Palau Communications has an ICT team that provides technical support to Government. • PILON respondents noted that there was very little local capability in cyber security. **Requirements and Standards** • The Palau Shipping Registry provides internationally developed guidelines for cyber security on-board ships.	• None identified to date.

Vigilant	**International Co-operation and Intel** • Part of United Nations, the Pacific Island Forum, and developing participating country of the Asia Development Bank (ADB). • Member of the Pacific Island Law Officers' Network (PILON). • Member of Pacific Cyber Security Operational Network (PaCSON). • Cyber incident response and investigation support has been provided by the FBI (from Hawaii / Guam) and/or the Australian Federal Police. **Detection and Monitoring** • None identified to date.	• None identified.
Resilient	**Connectivity and Redundancy** • Multiple ISPs – PalauNet (PNCC) and Palau Telecom. • Submarine cable – in operation since Dec 7 2017 (2018; BSCC). • Backup of satellites, with multiple upgrades to satellite capacity arrangements with O3b. **Cyber Incident Response (CERT)** • No CERT. **Cyber Crime Enforcement** • None identified to date. • Only 21 total police officers, most being part-time or dispatch officers.	• None identified.
Previous Cyber Incidents	Our conversations with in-country contracts identified no previous cyber security incidents based on anecdotal evidence.	

Key Cyber Risks – Palau



Papua New Guinea 

Key Thoughts
PNG is a relatively large country within the Pacific, with multiple submarine cables and an open telecommunications market. Representatives noted challenges with domestic connectivity/infrastructure, especially in providing fast and reliable internet to rural regions. PNG are in the process of centralising some Government systems though a US$53.3m grant from China for an integrated Government information system.

PNG have made some progress in managing cyber security risk, including implementing a cyber crime bill (2016), developing PNG's National Cybercrime Policy (2014), establishing leadership of cyber security with NICTA, and establishing PNG's CERT in 2018.

PNG faces the challenge of a large and disparate population, which will drive an ongoing need for effective awareness and outreach. In addition, due to their relative size there will be a need to provide standards/requirements which provide baseline coverage for a broad set of stakeholders (i.e. critical infrastructure and Government).

As high priority tasks, Papua New Guinea would benefit from:
- Build local capability through focused training and secondment opportunities.
- Uplift cyber security awareness and outreach to schools and communities.
- Establish guidance and standards to build a security baseline for projects involving critical infrastructure or central Government.

Population:
8,418,346 (2018; United Nations Department of Economic and Social Affairs: Population Division).

Key Economic Drivers:
- Natural resources / mining.
- Forestry.
- Fishing.
- Agriculture.

Connectivity:
- International: Multiple submarine cables (Teluk, Indonesia).

Broadband Uptake:
- Fixed Line: 0.2 per 100 inhabitants (2017; ITU).
- Mobile: 8.9 per 100 inhabitants (2017; ITU).
- Internet users: 9.6 per 100 inhabitants (2017; ITU).

Core Internet Uptake/Use Cases:
- Recreational.
- 380,000 Facebook users (4.8% penetration rate) (2016; internetworldstats).

Key Contacts:
- Minister for Communication and Information Technology – Hon. Jimmy Miringtoro.
- Attorney General – Davis Steven.

Key Institutions:
- The National Information Communication and Technology Authority (NICTA) – the lead agency for cyber security.
- Prime Minister's Office – have a dedicated security team.
- Department of Communication and Information.

Cyber Area	Current State	In-Progress / Planned

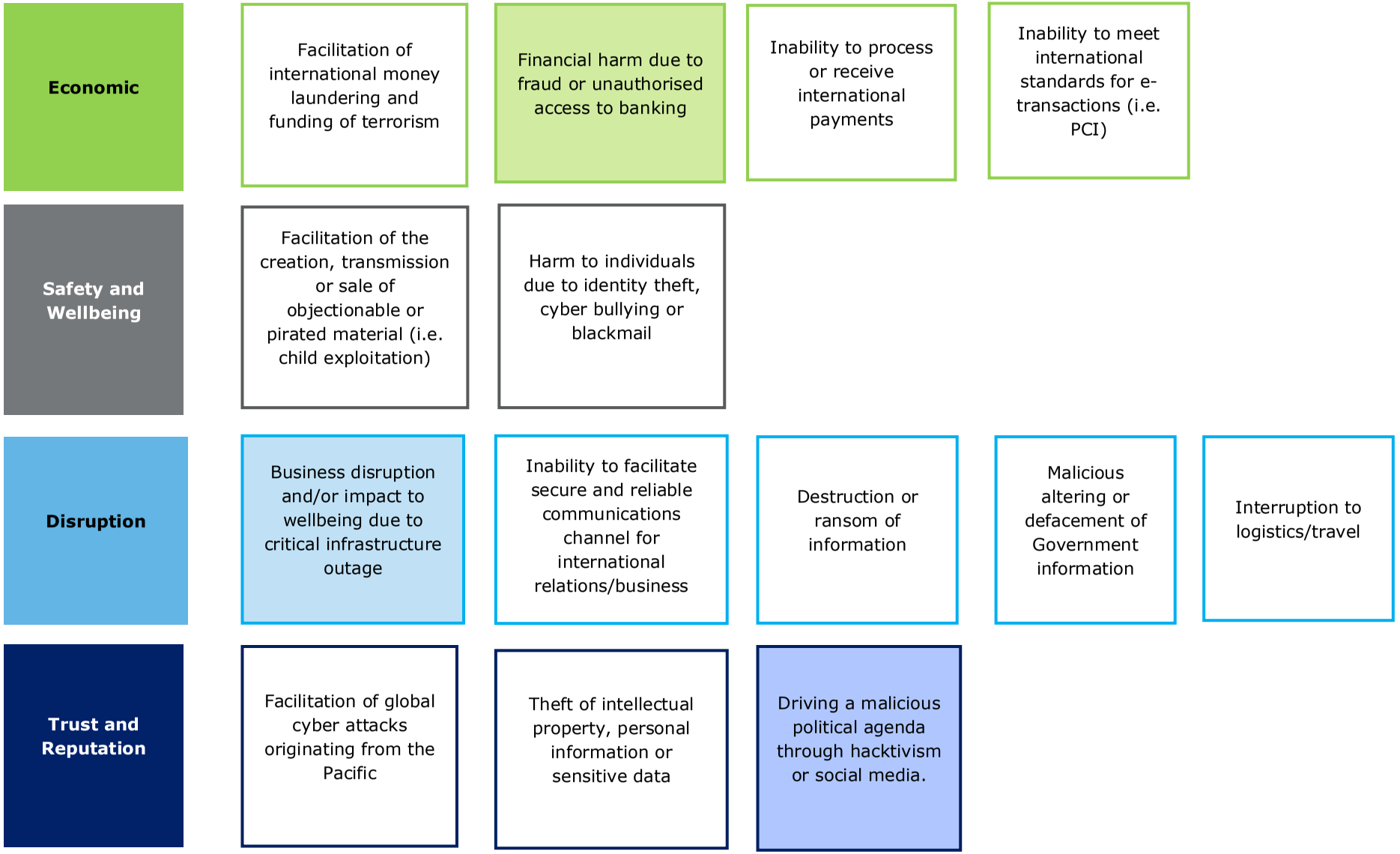
Strategy	**Strategy, Roadmap and Policy** • No overarching cyber security strategy. • National Cybercrime Policy was launched in October 2015. **Institutional Bodies** • The National Information Communication and Technology Authority (NICTA) is the lead for Cyber. • The Prime Minister's Office provide technical security expertise. • PNG and Australia worked together to establish a National Cyber Security Centre, focused on protecting critical information and infrastructure. • The PNG CERT provides technical and response/investigation support. **Training and Awareness** • PNG are a part of Cyber Safety Pasifika, which trains police officers to provide awareness and outreach on cyber security in their communities. **Risk Management** • None identified to date.	• Papua New Guinea has been developing a national cyber security policy and strategy. Public consultation on the strategy was invited and is expected to be addressed in 2018. • Recently received a grant from China of US$53.3m for an integrated Government information system.
Secure	**Legislation** The associated Chapman Tripp analysis outlines the following: • Cybercrime (substantive) – sophisticated. • Cybercrime (child protection) – established. • Cybercrime (procedural) – sophisticated. • Electronic transactions – none. • Privacy – initial. • Data protection – initial. • Digital authentication – initial. • Consumer protection – established. • Intellectual property – established. **Capability** • None identified to date. **Requirements and Standards** • None identified to date.	• There is an Electronic Transactions Act in draft, and a Data Protection Act has been proposed separately.

Vigilant	**International Co-operation and Intel** • Member of Pacific Islands Telecommunications Association, ITU IMPACT, Commonwealth Telecommunications Office (CTO). • Member of the APT and participates in APT organised forum on cyber security. • Member of the Pacific Island Law Officers' Network (PILON). • Member of Pacific Cyber Security Operational Network (PaCSON). • Member of the Pacific ICT Regulatory Resource Centre (PiRRC). • Receive assistance and funding from the Australian Federal Police (AFP) and Department of Foreign Affairs and Trade (DFAT). **Detection and Monitoring** • Mobile SIM card registration was enforced with a deadline of 31 January 2018.	• None identified to date.

Resilient	**Connectivity and Redundancy**
	• Multiple submarine cables.
	• Multiple ISPs, including:
	  ○ Digicel.
	  ○ BMobile.
	  ○ Telecom PNG.
	
	Cyber Incident Response (CERT)
	• PNG CERT was established in 2018. It is responsible for co-ordinating the management of cyber incident response, promoting cyber security and assisting with capacity building.
	
	Cyber Crime Enforcement
	• Royal Papua New Guinea Constabulary (in charge of cyber crime as well). Anecdotally, we are told the Police are not currently equipped to deal with cyber crime.
	• The Cybercrime Taskforce was established in 2014, but it is unclear if this has been effectively implemented.
	• Financial Action Taskforce (established for combating money laundering against terrorism).
		• None identified to date.

Previous Cyber Incidents	Our conversations with stakeholder representatives identified a number of previous cyber security incidents based on anecdotal evidence: • Online posts have been identified which provide guidance for "torturing sorcerers", which was identified to us as a sensitive cultural issue. The Police have been unable to prosecute the parties that created these posts. • An email server belonging to the PNG Government was breached, and a number of emails claiming to be from the PNG Government were sent out. In this case, no significant impact from these emails has yet been identified. • There have been reports of citizens that have fallen victim to online scams, specifically including sending money overseas to scammers.	

Key Cyber Risks – Papua New Guinea



Samoa 

Key Thoughts
Samoa is a country highly focused on being part of the connected world. While fixed-line broadband usage is declining, the total international bandwidth usage has grown by 20-30 times in the past 4 years, and mobile data usage is growing exponentially year-on-year. We were advised by representatives from the education sector that the second most popular subject in schools is Computer Studies.

Based on this cultural direction and its relative size in the region, Samoa has established some good baselines initiatives to uplift cyber security – with a strategy and key policies in place, strong institutional support from the Ministry of Communication and Information Technology (MCIT), and some requirements/standards and auditing in place for Government. We were able to identify some strong technical capability, but found this mostly isolated within the ISPs/Telcos. There is awareness about cyber security and related risks across Government, and potentially because of this, a number of known cyber security incidents have been identified and/or investigated.

As high priority tasks, Samoa would benefit from:

- The development of cyber crime capability within the Police (and/or MCIT), alongside enforcement protocols, that enable these entities to better investigate and enforce complaints relating to harassment, bullying, revenge porn, child porn and defamation using social media and other online services. In addition, in-progress updates to legislation should be completed to cover these areas in full.
- Stimulation of relationships between the private and public sectors, potentially driven by "as-a-Service" offerings from the private sector – which may help to bridge the gap between governance and the technical capabilities within the private sector.
- A better process for the public (and private) sectors to access skilled international resources.
- Additional access to ICT and cyber security education and training, from a school level upwards.

Population:
197,695 (2018; United Nations Department of Economic and Social Affairs: Population Division).

Key Economic Drivers:

- International remittance.
- Services.
- Agriculture.
- Forestry.
- Coconut products.
- Fishing.

Connectivity:

- International: Tui Samoa Cable.
- International: Hawaiki Cable (American Samoa).
- Local: 4G mobile.

Broadband Uptake:

- Fixed Line: 1 per 100 inhabitants (2017; ITU).
- Mobile: 29.8 per 100 inhabitants (2017; ITU).
- Internet users: 29.4 per 100 inhabitants (2017; ITU).

Core Internet Uptake/Use Cases:

- Mobile data (recreational) subscribers.
- 68,000 Facebook users (34.7% penetration rate) (2016; internetworldstats).

Key Contacts:

- Minister of Communications and Information and Technology – Hon. Afamasaga Lepuiai Rico Tupai.
- Attorney General – Lemalu Hermann Retzlaff.

Key Institutions:

- Ministry of Communication and Information Technology (MCIT).
- The National Information Communication and Technology Authority.

Cyber Area	Current State	In-Progress / Planned

Strategy

Strategy, Roadmap and Policy

- MCIT has released the Samoa National Cyber Security Strategy 2016-2021.
- The Communications Sector Plan 2017-2021 outlines a desire to centralise ICT capability.
- Samoa Government Internet & Email Policy 2016.
- Samoa Social Media Policy 2015.
- Memorandums of Understanding (MoUs) have been developed to formalise information sharing between some Government agencies.

Institutional Bodies

- MCIT has the overall responsibility for leading cyber security strategy and policy development.
- The National Information Communication and Technology Authority.

Training and Awareness

- APNIC provides technical training to staff who are responsible for the Samoa National Broadband Highway (SNBH).
- MCIT provides local training for technical staff within Government (covering some basic cyber security). They also provide awareness emails for Government staff.
- Cyber Safety Pasifika – including an annual cyber week for training and awareness in schools and communities.
- According to a representative from the Ministry of Education, Sport and Culture (MESC) - Computer Studies is the second most popular subject at schools, behind English, but there is a struggle to provide a good syllabus and teaching capacity.

Risk Management

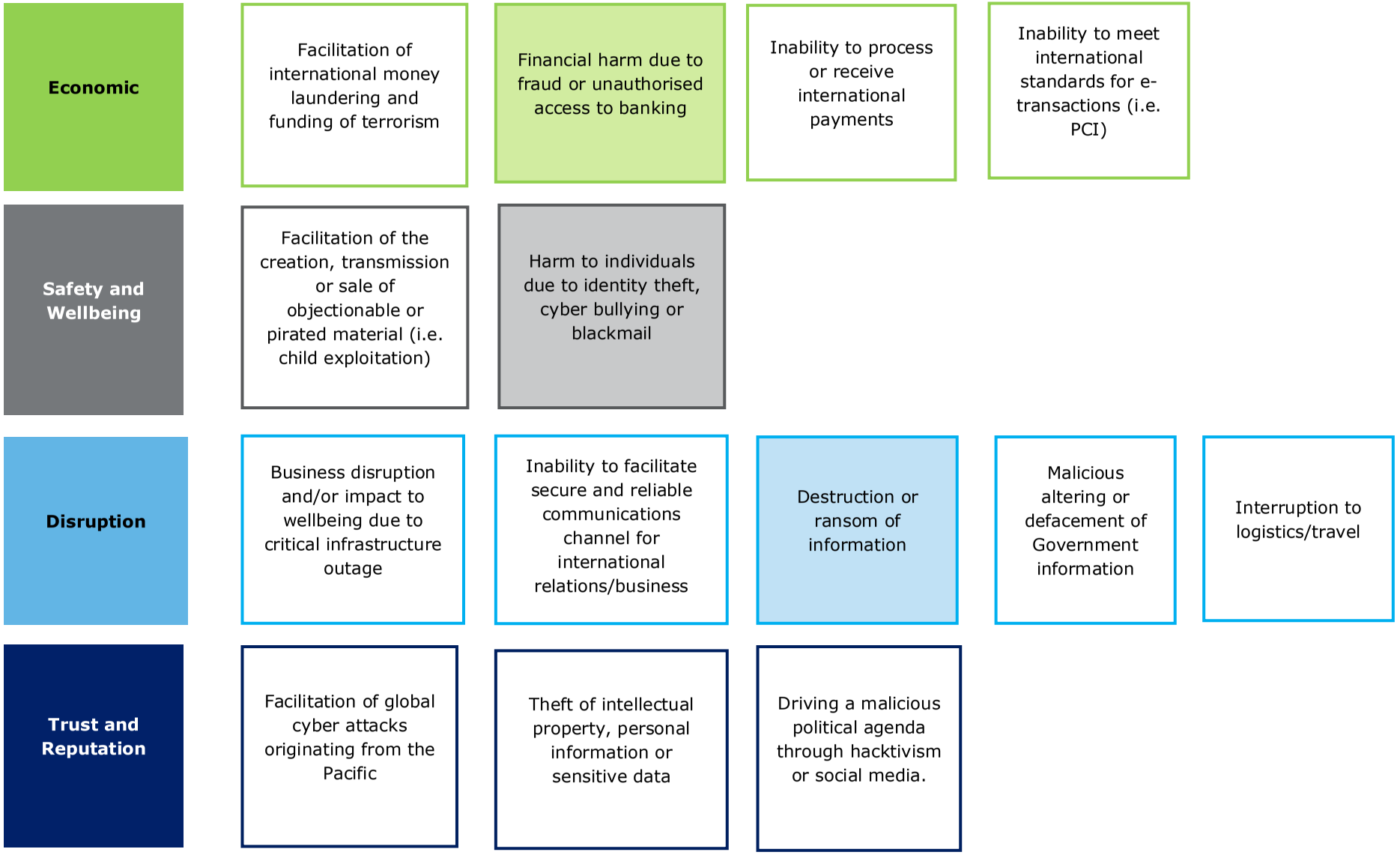
- The Samoa Audit Office has been running an IT audit programme for over 10 years, including some technical validation of cyber security controls (i.e. access and security of core Active Directory and the FinanceOne FMIS system).
- Disaster Recovery plans have been developed for core ICT systems.
- The University of Oxford has recently (April 2018) completed a Cybersecurity Capacity Review for Samoa, we identifies a number of Cyber risks and recommendations.
- National ICT Sector Plan proposed initiatives for establishing cyber security strategy and policies.
- Training on digital evidence and cyber crime prosecution is expected from the Council of Europe.
- Schools are working on implementing policy to take action against students who harass or bully others via social media or SMS.

Secure	**Legislation** The associated Chapman Tripp analysis outlines the following: • Cybercrime (substantive) – established. • Cybercrime (child protection) – established. • Cybercrime (procedural) – initial. • Electronic transactions – established. • Privacy – initial. • Data protection – initial. • Digital authentication – initial. • Consumer protection – established. • Intellectual property – established. **Capability** • Each Government agency uses their own ICT technical staff, but no specific cyber security capability has been identified. • Computer Services Limited (CSL, also known as SamoaNIC) provide ccTLD administration and ICT technical capability. • There is good cyber security capability and tooling within the local ISPs, BlueSky and Digicel. **Requirements and Standards** • The National ICT Committee (chaired by the PM) has oversight and approves all ICT projects for Government. When a project has a value of more than WST$50,000, specific procurement rules apply including provisions for maintenance, training and upgrades. • A minimum standard of TLS encryption is mandated for sites hosted on the e-Government network (SNBH) – however, we note that this is not in place for some Government sites. • Government policy dictates that agencies must have a firewall and use anti-virus (AV) on workstations and servers.	• Criminal Procedures Act 1972 is currently in review in regards to coverage of cyber security. • Money laundering changes are being made to prevent people promoting cryptocurrencies and not be considered financial institutions. • The Attorney General's Office has received a cabinet directive to ratify the Budapest Convention. • A National Identification scheme is in development.

Vigilant	**International Co-operation and Intel** • Member of the Pacific Island Law Officers' Network (PILON). • Member of Pacific Cyber Security Operational Network (PaCSON). • ITU and AusCERT have been engaged to assist with the development of a Samoa CERT. • Samoa have access to the Pacific Island ICT Regulatory Resource Centre (PiRRC). • CROP ICT group. • The Pacific Transnational Crime Coordination Centre (PTCCC) are providing threat intelligence for the region. • Council of Europe provide assistance in relation to acceding to the Budapest Convention. **Detection and Monitoring** • A Child Sexual Abuse Filtering system has been implemented by local ISPs. TCU and INTERPOL provide a blacklist of sites to local ISPs. • There has been requests made by regulators to the ISPs to block certain international sites – some of which have been executed. • All transactions to Nigeria have been blocked by the Central Bank – due to scams and fraud. • Law requires the ISPs to maintain SMS data and call metadata for a period of 7 years. • URLs accessed using fixed line and mobile data are maintained for a short period of time also, potentially 1-6 months. • There is currently no requirement for ISPs to retain digital evidence.	• None identified to date.
Resilient	**Connectivity and Redundancy** • MCIT is responsible for the Samoa National Broadband Highway (SNBH). Funded by a loan from China, this project has established a high-speed broadband network and data centre for e-Government, based near Apia and deployed in 2013. • Multiple internet cables. • Two main ISPs: Digicel and BlueSky. **Cyber Incident Response (CERT)** • No CERT but Samoa is creating one as per the Samoa National Cybersecurity Strategy. **Cyber Crime Enforcement** • The Samoa National Police Force has a good working relationship with the Australian Federal Police including for cyber crime.	• Samoa has requested ITU's assistance to establish a national CERT. • The Samoan Government is looking to migrate to Google's GSuite for resilience. • There is a plan to complete the Manatua Submarine Cable by 2019, which will further connect Samoa, Cook Islands, Niue, French Polynesia and Samoa.

Previous Cyber Incidents	Our conversations with stakeholder representatives identified a number of previous cyber security incidents based on anecdotal evidence: • Skimming devices have been identified on ATMs, and the reports of these devices being found have been increasing. Specifically, a Romanian national was prosecuted (in 2018) in relation to ATM skimming. This prosecution was facilitated by a tip from Tonga. • There has been an increase in reports of online fraud and scams (including WST$50k that was stolen from a citizen by a Nigerian via Western Union). • Cryptocurrency mining malware has been discovered and removed from some Government workstations. • There has been a significant amount of harassment and bullying using social media, including successful prosecutions. A number of parties noted that an improved ability to work with Facebook is required to manage these. • There have been 3 major cases of defamation via social media, where there has been no capability to successfully obtain information from Facebook. • There have been a number of reports of 'revenge porn', which is not covered by existing legislation. • The Ministry of Finance suffered a ransomware attack, through which a small amount of data was lost. • A number of significant phishing campaigns (via phone calls) have been identified coming from Eastern Europe. • SIM bypass attacks have been identified – using fake cell towers to facilitate arbitrage on international calling. • A number of DDoS attacks have been identified, of various scales and against various targets. Some have been effective – i.e. in taking down the mobile network for several hours. • There have been a number of successful attacks on local websites. • There have been a number of attacks that impacted private automatic branch exchange (PABX)/Voice over Internet Protocol (VoIP) phone systems. Attackers gain access to these systems and then use them to phone toll numbers they control. There have been a number that have incurred losses of WST$40k+.

Key Cyber Risks – Samoa



Solomon Islands 

Key Thoughts
The Solomon Islands have had historical connectivity limitations with no submarine cable in place, and the closed telecommunications market (until late 2009). The opening of the market (now there are 3 main providers – regulated by TCSI) and increasing demand has resulted in an increase in mobile data subscribers from ~8,000 in 2010 to ~115,000 in 2017 (TCSI website). In parallel, the Solomon Islands has embarked on an e-Government project, centralising the network and infrastructure (SIG CONNECT) with the support of the SIG ICT Support Unit and Australian advisors. This project is well progressed (functioning in production), and uptake has been good.

With the rapid increase in the use of technology and connectivity, growth pains are evident in the Solomon Islands. This manifests itself in the institutional structure and ownership of governance, capabilities and actions relating to ICT and cyber security. While there are a number of key institutions, the demarcation of roles and ownership of actions are unclear – and there are opportunities to make the operating model more efficient/effective. This is recognised by the stakeholders, and the National ICT Policy outlines a need to establish another institution and a Chief Information Officer for Government.

From a risk perspective, there have been international cyber security attacks and scams with a digital footprint originating in Solomon Islands' controlled digital space (+677 area code and IPs addresses originating from Solomon Islands). In addition, our in-country consultations identified an emphasis on citizens being impacted by both international cyber scams and bullying, harassment and exploitation via social media and similar services. The legal framework and investigation/enforcement capabilities to support the prosecution or mitigation of these events is not in place.

As high priority tasks, The Solomon Islands would benefit from:

- A clear leader, with an appropriate level of seniority with-in Government, to drive cyber security and maintain momentum with the rapid expansion of connectivity.
- The development and execution of a national cyber security strategy, which should include consideration for how roles, responsibilities and institutional structure can be streamlined and clarified.
- The development and implementation of cyber crime legislation which aligns with the Budapest Convention, alongside enforcement protocols and training for investigation and enforcement.
- Establishing a Security Operations Centre (SOC) / CERT capability to support cyber security vigilance, incident response and reporting, and provide a central point for cyber capability.

Population:
623,281 (2018; United Nations Department of Economic and Social Affairs: Population Division).

Key Economic Drivers:

- Gold mining.
- Agriculture.
- Fishing.
- Tourism.
- Forestry (logging).

Connectivity:

- International: O3B Satellite Uplink.
- Local: 3G mobile covering ~93% of land area.
- Local: Fixed line is provided by Solomon Telekom (Our Telekom).

Broadband Uptake:

- Fixed Line: 0.2 per 100 inhabitants (2017; ITU).
- Mobile: 18.6 per 100 inhabitants (2017; ITU).
- Internet users: 11 per 100 inhabitants (2017; ITU).

Core Internet Uptake/Use Cases:

- Mobile data (recreational).
- Mobile banking.
- 41,000 Facebook users (6.8% penetration rate) (2016; internetworldstats).

Key Contacts:

- Minister for Communication and Aviation – Hon. Peter Shanel Agovaka.
- Director of Information, Communication and Technology Support Unit (ICTSU).
- President of the ITSSI.
- Minister for Police, National Security and Correctional Services – Hon. Sam Shemuel Iduri.
- Telecommunications Commissioner (TCSI).
- Attorney General – James Apaniai.

Key Institutions:

- Ministry of Communication and Aviation (MCA).
- Solomon Islands Government ICT Support Unit (SIG ICTSU – a division of the Ministry of Finance & Treasury).
- Telecommunications Commission of Solomon Islands (TCSI).
- Information Technology Society Solomon Islands (ITSSI).
- Central Bank of Solomon Islands (CBSI).
- Royal Solomon Islands Police Force (RSIPF).
- Ministry of Police, National Security and Correctional Services.
- Ministry of Justice and Legal Affairs.

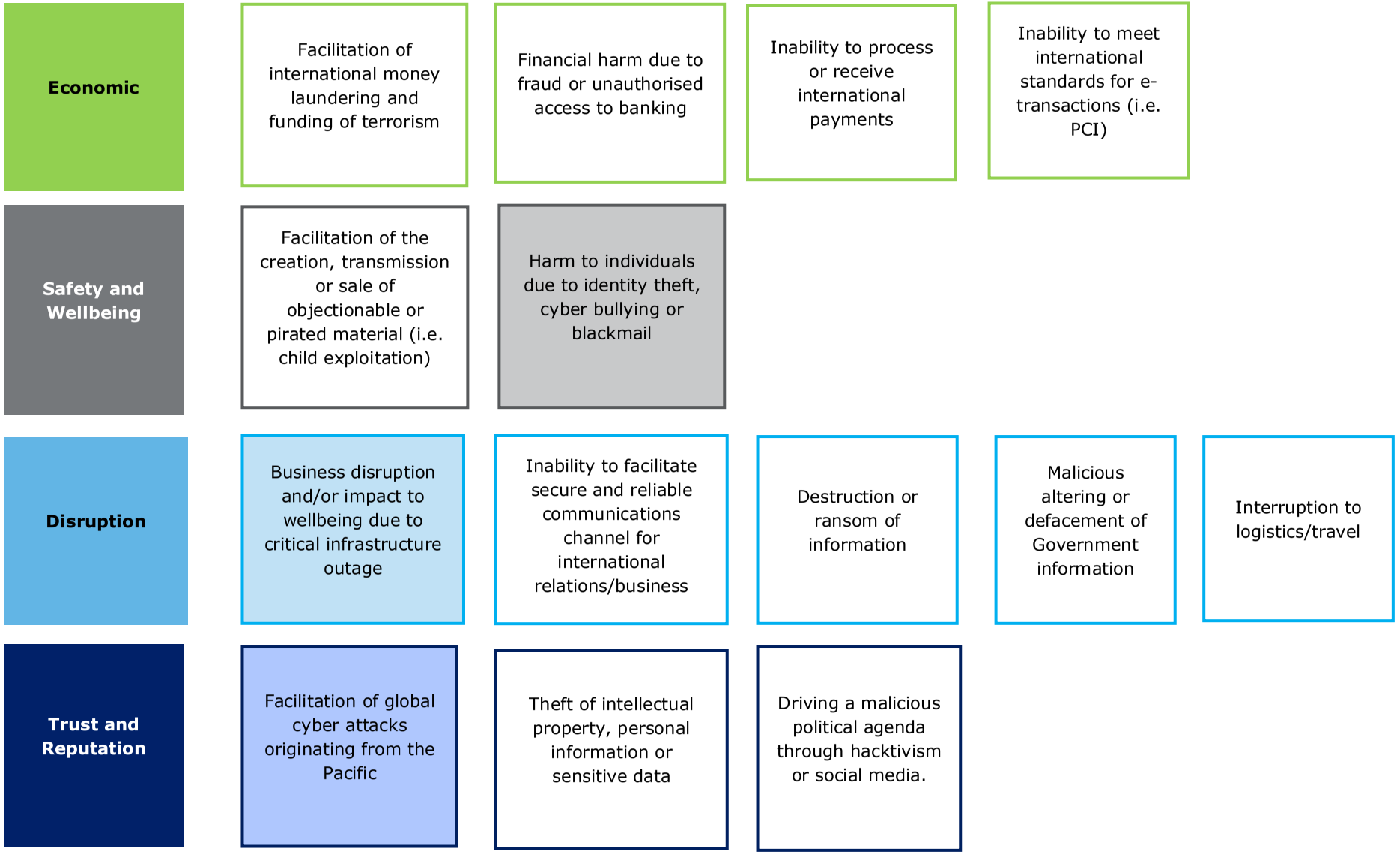
Cyber Area	Current State	In-Progress / Planned

Strategy	**Strategy, Roadmap and Policy** • The National ICT Policy, launched 2017 – which mentions cyber security, and outlines a need to establish a National Information Office and a Chief Information Officer to lead it. • The Government of Solomon Islands has acknowledged that improving ICT sector needs to be a priority and has addressed this in its National Development Strategy 2016-2035. • CBSI has its own IT Security Policy. **Institutional Bodies** • MCA – holds overall responsibility for cyber security. • SIG ICTSU – provides core technical subject matter expertise for ICT and cyber security. • ITSSI – provides policy advice, technical capability, awareness, and supports staff and citizens for ICT and cyber security. • TCSI – oversees telecommunications; including radio spectrum, price control, consumer complaints, licensing and administrator of the Telecommunications Act 2009. TCSI is the conduit for requesting digital evidence, and implementing controls, relating to the ISPs. Also, informally responsible for incident reporting/aggregation. • Solomon Telekom – administers the CCTLD. **Training and Awareness** • ITSSI runs Government-focused workshops and awareness campaigns on cyber security, alongside the annual National ICT Week – which includes public events and schools. • First 'Girls in ICT' Day held – which identified significant interest, but also a number of attendees noted that bullying and harassment over social media was a major issue. **Risk Management** • None identified to date. **Privacy** • The potential over-sharing of information between Justice, Corrections and Police was identified as a risk. • Government sharing of information is not well formalised, and currently relies on a string of MoUs. • Citizens have a constitutional right to privacy.	• The PILON Strategic Plan 2016-2018 has recognised cyber crime as a priority issue for Pacific Islands, and the Solomon Islands are engaging with cyber crime initiatives as a part of the PILON agenda/membership. • SIG ICTSU has developed a request for tender for a security audit on e-Government infrastructure. • The Attorney General's Office has proposed and are pursuing the implementation of a National Cyber Security Task Force (made up of RSIPF, AG, DPP, ICTSU, MCA), to deliver cyber crime legislation and strategy. • The MCA may absorb the ICTSU, as it is more aligned with the responsibilities of this Ministry. • MCA and ICTSU are working on a National ICT Implementation Plan to sit underneath the existing ICT policy.

Secure	**Legislation** The associated Chapman Tripp analysis outlines the following: • Cybercrime (substantive) – initial. • Cybercrime (child protection) – none. • Cybercrime (procedural) – initial. • Electronic transactions – none. • Privacy – initial. • Data protection – none. • Digital authentication – none. • Consumer protection – initial. • Intellectual property – none. **Capability** • The SIG ICTSU has 15 full-time staff and acts as a technical and policy advisor to Government for ICT and basic cyber security. • DFAT have been providing two long-term advisors for the ICSTU and SIG CONNECT – one technical, one strategy focused. • All-of-Government network and systems (e-Government) are provided and supported by ICTSU and Solomon Telekom. This includes patching/maintenance, anti-virus, secure software builds, filtering/firewalls and centralised identity management. • CBSI have their own ICT systems and team, including staff trained to post-graduate level in cyber security. • Solomon Water utilise Industrial Control Systems (ICS), and have implemented upgraded firewalls, restrictions on access and their own IT Security Policy. • The RSIPF have an officer trained in core digital forensics. • MCA has a policy unit who played a major role in developing the National ICT Policy (only 3 people). **Requirements and Standards** • The SIG ICTSU issued minimum procurement standards for Government, but these have ceased since April 2014. • There are no requirements or guidelines for ISPs to maintain digital evidence/records, but currently are maintaining SMS data indefinitely.	• Additional legislation initiatives that are in-progress are outlined within the associated Chapman Tripp report.
Vigilant	**International Co-operation and Intel** • The Australian Government (DFAT) is providing long term advisors and funding in relation to connectivity (it will fund the new submarine cable), technical ICT/cyber and policy/strategy. • Member of the Pacific Island Law Officers' Network (PILON). • Member of Pacific Cyber Security Operational Network (PaCSON). • Member of Pacific Islands Telecommunications Association (PITA). • Member of the International Telecommunications Union (ITU). **Detection and Monitoring** • Although not mandated to do so, ISPs are storing SMS data and call metadata.	• The MOF/ICTSU has received/confirmed funding from DFAT to build cyber security capability and setup a Security Operations Centre (SOC) for Government.

Resilient	**Connectivity and Redundancy** • International bandwidth is provided by O3B satellites. • All-of-Government SIG-CONNECT network and infrastructure provided by Solomon Telekom and SIG ICTSU. A disaster recovery site has been setup on Guadalcanal. • Multiple local ISPs: - Solomon [Our] Telekom. - bmobile-Vodafone. - Satsol Limited. **Cyber Incident Response (CERT)** • The Solomon Islands was a member of PacCERT (now closed). • No existing CERT. **Cyber Crime Enforcement** • None identified to date.	• The Solomon Islands Submarine Cable Company is in charge of preparing to connect to a new subsea cable which will be built with support and funding from Australia by the end of 2019.
Previous Cyber Incidents	Our conversations with stakeholder representatives identified a number of previous cyber security incidents based on anecdotal evidence: • A significant number of citizens have been impacted by scams and fraud executed via the internet. • There have been some reports of people sharing inappropriate images of young people, and/or 'revenge porn'. • There have been reports of scams originating from the Solomon Islands country code (+677), but the source has not yet been identified. • A person stored and shared inappropriate pictures of their ex-partner from a work device, but prosecution of this person was not achieved due to an inability to properly investigate. • A telcos IP address range has been identified as the source of international cyber security attacks – including an attack against a Welsh bank (reported by INTERPOL). • DDoS attacks have been observed to disrupt services in the Solomon Islands. • Malware has been found on Government workstations (mostly staff clicking malicious links). • SIM bypass attacks – unlicensed operators using fake cell towers to make money off routing international calls.	

Key Cyber Risks – Solomon Islands



Tonga 

Key Thoughts
The Southern Cable, which enables high speed international connectivity for Tonga, was connected in 2013 – driving significant uptake of technology-based services and opportunities in Tonga. The Tongan Government has established core e-Government infrastructure (including two local datacentres), and there has been significant uptake of social media across citizens.

Tonga has made significant advancements toward improving its ability to identify and address cyber crime and resilience concerns. These advancements include establishing cyber crime legislation (and acceding to the Budapest Convention), establishing top-level governance, launching a local CERT, and a clear focus on international collaboration across the Pacific region.

As high priority tasks, Tonga would benefit from:

- Establish its core Cyber strategy / action plan – which should focus on maintaining current momentum (include driving sustainability in existing projects), further define ownership and responsibility for cyber security, support the successful implementation of cyber crime legislation/enforcement, and should also encourage continued sharing across the region.
- Establish greater capability and avenues for local law enforcement to respond to cyber crime, including the establishment of an enforcement protocol which outlines clear processes for working with local ISPs/institutions, international partners, and social media.
- Expand their CERT resource base, especially in the medium term, to help them build on the model it has created and to share this with the wider region.

Population:
109,008 (2018; United Nations Department of Economic and Social Affairs: Population Division).

Key Economic Drivers:

- International Remittances
- Handicrafts (3% of GDP).
- Agriculture.
- Tourism.
- Fishing.
- Construction.

Connectivity:

- International: Submarine Cable (to Fiji), branches from Tongatapu to Pangai and Neiafu (as at 2015, was providing 600mbps).

Broadband Uptake:

- Fixed Line: 1.7 per 100 inhabitants (2017; ITU).
- Mobile: 56 per 100 inhabitants (2017; ITU).
- Internet users: 40 per 100 inhabitants (2017; ITU).

Core Internet Uptake/Use Cases:

- Mobile data (recreational) subscribers.
- 43,000 Facebook users (39.9% penetration rate) (2016; internetworldstats).

Key Contacts:

- CEO – Ministry of Meteorology, Energy, Information, Disaster Management, Climate Change and Communications (MEIDECC).
- Director of Tonga CERT.
- Minister for Infrastructure and Tourism – Hon. Semisi Sika.

Key Institutions:

- Tonga CERT.
- Ministry of Meteorology, Energy, Information, Disaster Management, Climate Change and Communications (MEIDECC) / Ministry of Information and Communications (MIC).
- Royal Tonga Police
- Attorney General's Office.
- Cyber Challenges Task Force (CCTF).

Cyber Area	Current State	In-Progress / Planned

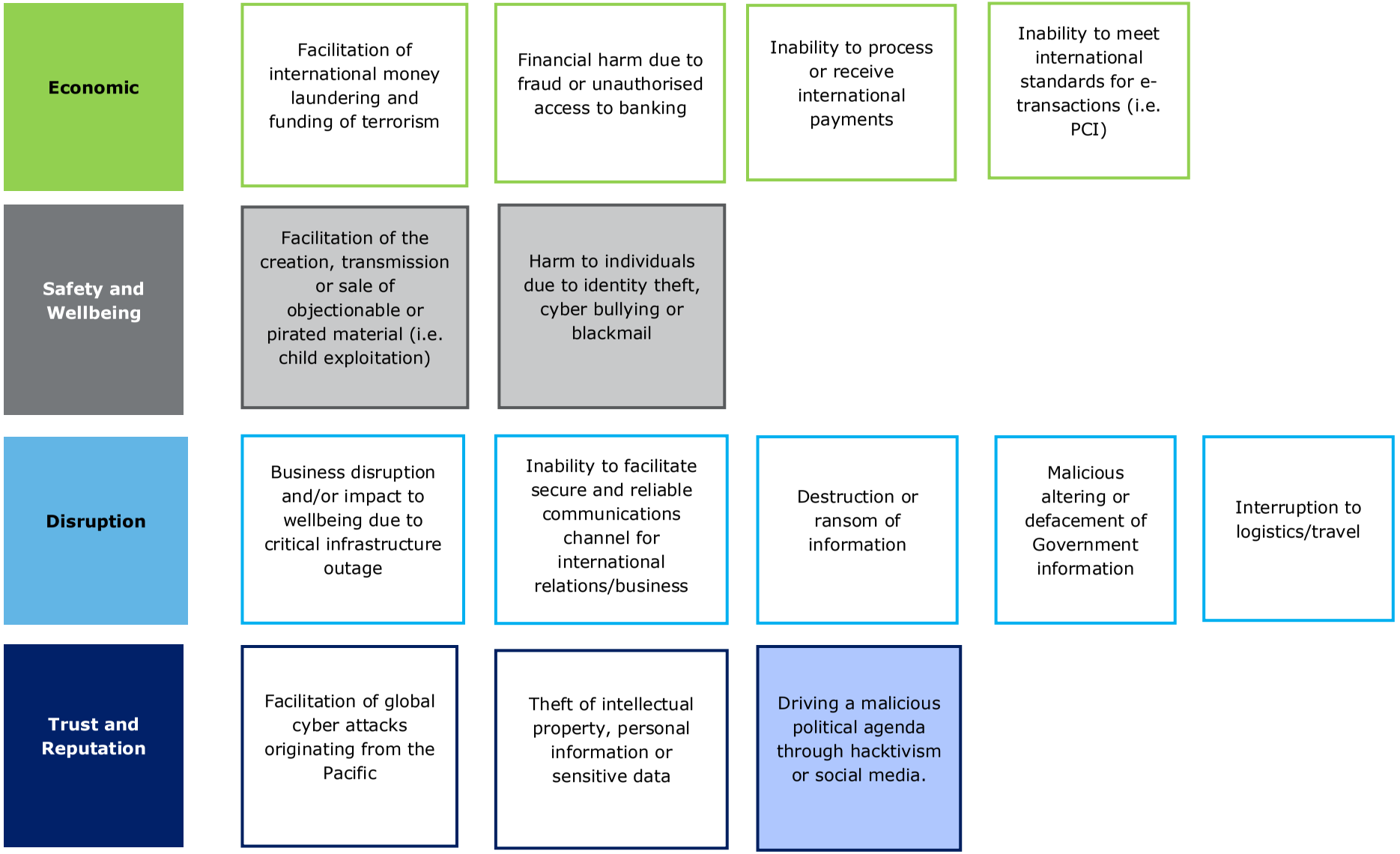
Strategy	**Strategy, Roadmap and Policy** • No overarching cyber security strategy. • A National ICT Policy was developed and implemented in 2009 (now outdated). **Institutional Bodies** • MEIDECC is the lead agency for cyber security. • Cyber Challenge Task Force (established in 2013) has three working committees for cyber safety, cyber security and cyber crime. • Tonga established a local CERT (2016). **Training and Awareness** • Cyber crime public consultation funded by ICB4PAC (2013). • MOU with Netsafe to help the Government provide a safer cyber experience for citizens. • Pacific Island Law Officer's Network (PILON) Cybercrime Workshop (2017) and PILON Cybercrime Working Group Meeting (2018). • Cyber Safety Pasifika training and awareness for Police and communities. **Risk Management** • None identified to date.	• The Cyber Challenge Task Force has been tasked with formulating national cyber crime and cyber security strategies.
Secure	**Legislation** The associated Chapman Tripp analysis outlines the following: • Cybercrime (substantive) - established • Cybercrime (child protection) – established. • Cybercrime (procedural) – established. • Electronic transactions – none. • Privacy – initial. • Data protection – initial. • Digital authentication – initial. • Consumer protection – established. • Intellectual property – established. **Capability** • Tonga CERT has technical cyber security capabilities (although constrained by resourcing). • Tonga has local legal capability and experience relating to cyber security both in the private sector and within their Attorney General's office. **Requirements and Standards** • None identified to date.	• Additional legislation initiatives that are in-progress are outlined within the associated Chapman Tripp report.

Vigilant	**International Co-operation and Intel** • Tonga has acceded to the Budapest Convention on Cyber crime. • Framework of Operational Understanding on cyber security (collaboration between CERT Aus and CERT Tonga). • Member of Pacific Islands Telecommunications Association (PITA), ITU IMPACT, Commonwealth Telecommunications Office (CTO), Pacific Island Law Officers' Network (PILON), Pacific Cyber Security Operational network (PaCSON). • Restricted member of INTERPOL. • Memorandum of Understanding (MoU) with AUSTRAC and Australian Federal Police for sharing information. • MoU between the Tongan Government and Waikato University to collaborate on cyber security issues. • MoU signed with Netsafe in New Zealand to help the Tongan Government provide a safer online experience for citizens. • Global Action Taskforce on Cybercrime Plus (GLACY+ Project). **Detection and Monitoring** • None identified to date.	• None identified to date.

Resilient	**Connectivity and Redundancy**
	• International submarine cable through Fiji.
	• Tonga Communications Corporation provides access to international bandwidth.
	• Multiple local ISPs:
	  ○ Tonga Communications Corporation
	  ○ Digicel Tonga.
	• Department of Communications regulates telco service providers.
	
	Cyber Incident Response (CERT)
	• Tonga has established a national CERT – TongaCERT (CERT.to).
	
	Cyber Crime Enforcement
	• None identified to date.
		• None identified to date.

Previous Cyber Incidents	Our conversations with stakeholder representatives have identified a number of previous cyber security incidents based on anecdotal evidence: • Reports of cyber bullying, harassment and transfer of illicit images of children (citing social media as a possible catalyst/facilitator). • Reports of ATM card skimming. • Numerous core Government sites have been blacklisted for potential malicious activity – indicating they may have weak security controls or malware infections.	

Key Cyber Risks – Tonga



Tuvalu 

Key Thoughts
Tuvalu is one of the least connected countries in the region today, with access to ICT services and connectivity extremely limited outside the main island of Funafuti. International connectivity is further limited by the lack of a submarine cable, and no compensating coverage being provided from the O3B satellite network (other satellite connectivity is available). The in-progress Tuvalu Telecommunications and ICT Development Project (assisted by the World Bank) will aim to address international and domestic connectivity through a public-private partnership and installation of a submarine cable. Digital payments are very limited in Tuvalu, according to the representatives we met there are no ATMs or credit cards readily available. In addition, online or text-message banking is not available. We were informed that banks would authorise payments based on email, but only if a physical signature was attached.

Consider their relatively small population and low connectivity, Tuvalu have taken some initial steps towards managing cyber security risk. In particular, draft legislation for cyber crime has been developed, and two officers within the Tuvalu Police Force have been assigned to support cyber crime cases. Tuvalu are a part of Cyber Safety Pasifika and have completed a public cyber security awareness campaign in 2015. They are also part of PaCSON, which is targeted at building technical cyber security pacific (and providing support) through collaboration among other Pacific countries.

As high priority tasks, Tuvalu would benefit from:
- Formalise institutional ownership of cyber security, and develop an associated strategy and work plan.
- Complete the implementation of cyber crime law, including providing training to enforcement and the judiciary.
- Establish a formal international/regional partnership which supports cyber security incident response and investigation support.

Population:
11,287 (2018; United Nations Department of Economic and Social Affairs: Population Division).

Key Economic Drivers:
- Sale of fishing rights.
- International remittance.
- Lease of top level domain (.tv) – 10% of GDP.

Connectivity:
- International: satellite.
- Local: 3G launched in 2013. TTC launched a 4G service in 2018.
- No submarine cable.

Broadband Uptake:
- Fixed Line: 8.2 per 100 inhabitants (2016; ITU).
- Mobile: 4,000 (2015; BuddeComm).
- Internet users: 46 per 100 inhabitants (2016; ITU).

Core Internet Uptake/Use Cases:
- Recreational.
- 2,300 Facebook users (23.1% penetration rate) (2016; internetworldstats).

Key Contacts:
- Minister of Works, Transport and Communication.
- Attorney-General.

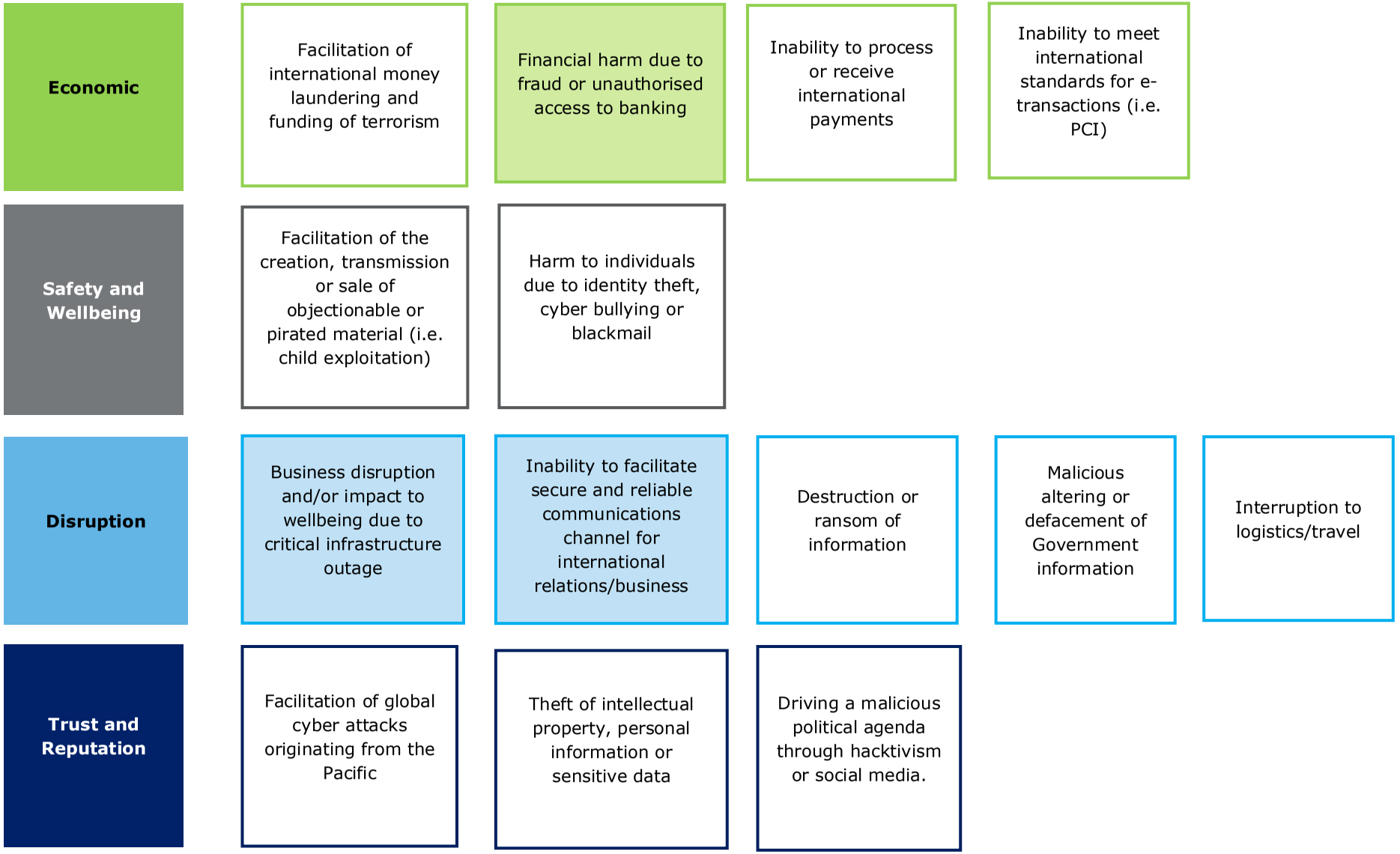
Key Institutions:
- Ministry of Works, Transport and Communication.
- ICT Department of the Government of Tuvalu.
- Tuvalu Police Force.
- Attorney General's Office.
- Tuvalu Telecommunications Corporation (TTC).

Cyber Area	Current State	In-Progress / Planned

Strategy	**Strategy, Roadmap and Policy** • No cyber security strategy. • The Government of Tuvalu outlined in its National Development Plan (NDP) 2016-2020 the key role of ICT services as an underpinning enabler for development in its areas of priority, such as education, health, and disaster management. The implementation of eGovernment is included within this strategy. • There is evidence of a National ICT Policy (2017), but we have been unable to locate it. **Institutional Bodies** • Ministry of Works, Transport and Communication (MCT) – responsible for development of ICT policy. MCT are currently prioritising eGovernment work, installation of a submarine cable, and the Cyber Crime Bill. • Department of ICT. • Tuvalu Police Force. **Training and Awareness** • An awareness campaign for Government staff was completed in 2015. • AFP has provided training to a limited number of officers from the Tuvalu Police Force as a part of the Cyber Safety Pasifika programme. **Risk Management** • None identified to date.	• The Tuvalu Telecommunications and ICT Development Project proposes support for Tuvalu to enable the environment for improved telecoms/ICT provision, a restructured market and a sustainable solution for connectivity.
Secure	**Legislation** The associated Chapman Tripp analysis outlines the following: • Cybercrime (substantive) - initial • Cybercrime (child protection) – none. • Cybercrime (procedural) – initial. • Electronic transactions – none. • Privacy – initial. • Data protection – none. • Digital authentication – none. • Consumer protection – none. • Intellectual property – initial. **Capability** • None identified to date. **Requirements and Standards** • None identified to date.	• Draft legislation covering cyber crime has been developed and is awaiting feedback, endorsement and implementation. This has been supported by international consultants and funding.

Vigilant	**International Co-operation and Intel** • Tuvalu has recognised partnerships with ITU and PiRRC. • Member of the Pacific Islands Law Officers' Network (PILON). • Member of the Pacific Cyber Security Operational Network (PaCSON). • A network-sharing deal was signed between Tuvalu and FSM in 2015. • The Australian Federal Police provide cyber-related training and awareness, including as a part of Cyber Safety Pasifika. **Detection and Monitoring** • None identified to date.	• None identified to date.
Resilient	**Connectivity and Redundancy** • TCC is a state-owned enterprise, which provides fixed line telephone communications to subscribers on each of the islands of Tuvalu. **Cyber Incident Response (CERT)** • Previously a member of PacCERT. • No current CERT. **Cyber Crime Enforcement** • The Tuvalu National Police Force and the Department of Information and Communication handle reports of cyber crime. Two officers have been designated to handle such cases.	• Tuvalu has expressed a desire to connect to an international submarine cable (i.e. Southern Cross). • The Kacific-1 satellite (planned to be live in 2019) will provide additional bandwidth for Tuvalu – circa 80-150Mbps. • The Tuvalu Telecommunications and ICT Development Project, with help from the World Bank, will reform the Tuvalu Telecoms Corporation and redevelop it into a public-private partnership. In addition, the project will support the installation of a submarine cable.
Previous Cyber Incidents	Our conversations with stakeholder representatives have identified a number of previous cyber security incidents based on anecdotal evidence: • A citizen sent ~NZ$500,000 to a scammer who was purporting to offer a return on this investment. The citizen had to take out a loan for the majority of this money.	

Key Cyber Risks – Tuvalu



Vanuatu 

Key Thoughts
Vanuatu is a relatively highly connected Pacific Island nation with their Universal Access Policy driving internet connectivity to approximately 98% of the population. This connectivity is supported by the international submarine cable running through Fiji. The Vanuatu Government has progressed central eGovernment deployment by establishing a private high-speed network in Port Vila and forming the Office of the Government Chief Information Officer (OGCIO). Debit and credit card penetration in Vanuatu is further progressed than a number of other Pacific Island countries, and many stores accept card payments, but online transactions are still low.

Vanuatu is relatively progressed (from a regional perspective) in managing cyber security risk. A number of interviewees attributed this progression to a previous Prime Minister who drove ICT and cyber security as priorities for Government. They have established their local CERT (overseen by the OGCIO) in 2018. The CERT includes three capable staff with international training in technical cyber security and governance. They have been executing a number of tasks on behalf of the Vanuatu Government, including: vulnerability scanning, penetration testing, security design assistance, policy and strategic support, incident response and reporting, and developing institutional operating models/governance. The CERT is supported by a number of key institutions including the Telecommunications Radiocommunications and Broadcasting Regulator (TRBR) and the Vanuatu/Pacific Internet Governance Forum (IGF). They are actively considering further key governance institutions, most notably the proposed "Vanuatu Research and Development Unit" who would focus on smart procurement of ICT and security products – confirming they are adequately supported and fit-for-purpose in terms of local requirements. This institution would address a critical challenge in ongoing ICT and cyber security projects.

Based on Vanuatu's relative progression in cyber security (including the establishment of the local CERT), they are aware of a number of incidents and in many cases have successfully prosecuted cyber criminals (i.e. for fraud, child exploitation and sharing online, etc). Cyber bullying and child exploitation was noted as a high risk, as evidenced by a number of incidents, prosecutions and reports. Key challenges in regards to a lack of computer literacy generally and in the Police, legislative and enforcement deficiencies, and a lack of access to training and funding were outlined consistently. In addition, there has been a lot of activity in the ICT and cyber security space, but this needs to be consolidated under a single institution and single strategy/plan.

Finally, there is a higher desire for privacy legislation/protection in Vanuatu than a number of Pacific Islands, and as such there has been consideration of privacy legislation by the Ministry of Justice.

Based on the location, capability and relative maturity of Vanuatu, we propose that Vanuatu would be a good candidate for the establishment of a physical base for regional cyber security initiatives.

As high priority tasks, Vanuatu would benefit from:
- Complete the development of the National Cyber security Strategy, and consolidate Cyber activities formally under a single institution / leader.
- Develop and implement fit-for-purpose cyber crime legislation, and provide training to the Judiciary and Police.
- Provide additional support to the OGCIO / Vanuatu CERT to help them continue to assist and share locally and with other Pacific Island countries.

Population:
282,117 (2018; United Nations Department of Economic and Social Affairs: Population Division).

Key Economic Drivers:
- Agriculture.
- Tourism.
- Offshore financial.
- Beef farming (cattle).

Connectivity:
- International: Interchange Submarine cable (linking Vanuatu to Fiji).
- International: O3B satellite backup.
- Local: eGovernment private broadband infrastructure.

Broadband Uptake:
- Fixed Line: 1.8 per 100 inhabitants (2017; ITU).
- Mobile: 45.5 per 100 inhabitants (2017; ITU).
- Internet users: 24 per 100 inhabitants (2017; ITU).

Core Internet Uptake/Use Cases:
- Recreational.
- 34,000 Facebook users (12.3% penetration rate) (2016; internetworldstats).

Key Contacts:
- Minister for Justice – Hon. Ronald Warsal.
- Attorney General – Ishmael Kalsakau.
- Office of the Government Chief Information Officer (OGCIO) – Fred Samuel.

Key Institutions:
- Vanuatu CERT.
- Ministry of Justice.
- The Office of the Government Chief Information Officer (OGCIO).
- Telecommunications Radiocommunications and Broadcasting Regulator (TRBR).
- Pacific Internet Governance Forum (Pacific IGF) and the local Vanuatu IGF.

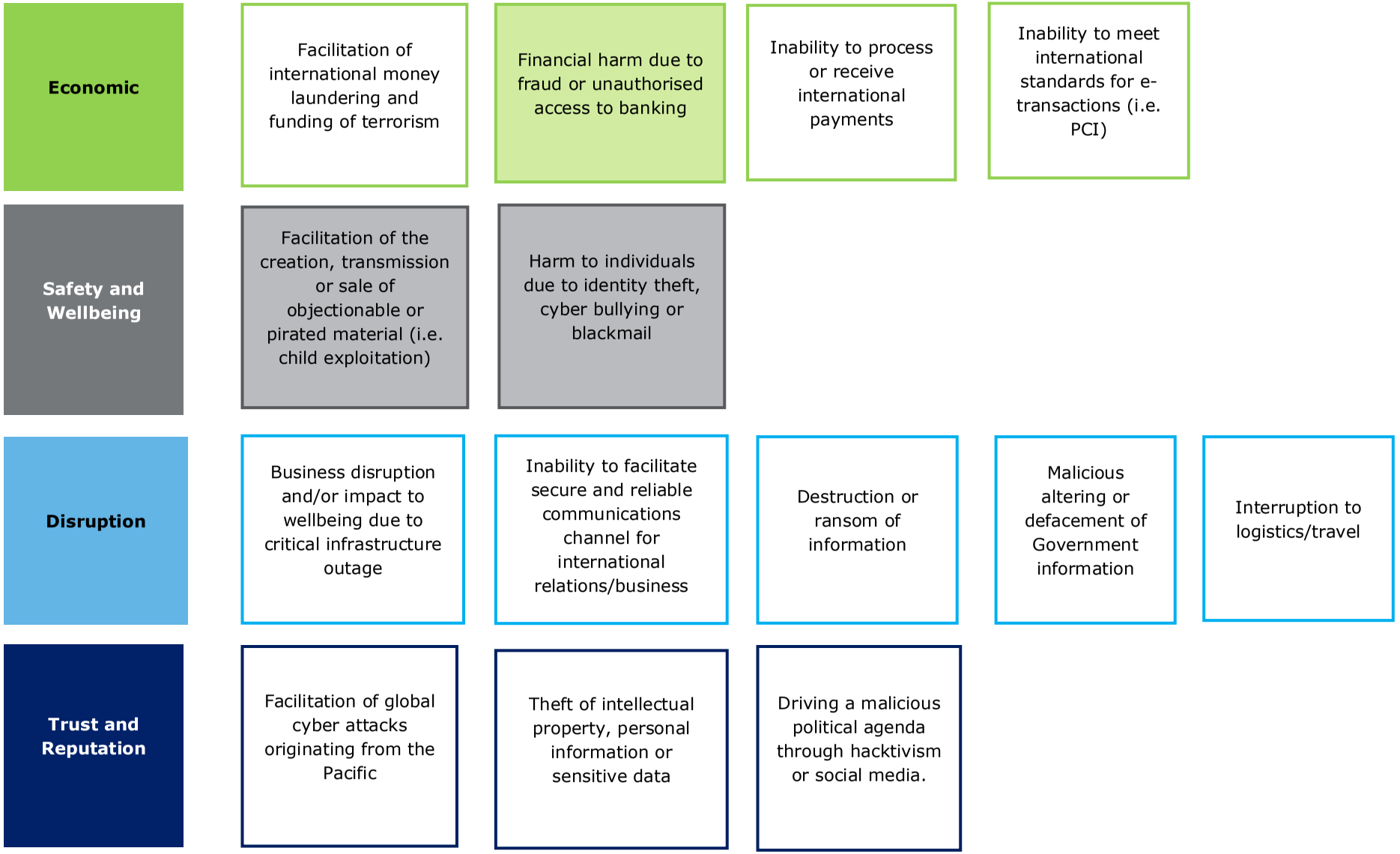
Cyber Area	Current State	In-Progress / Planned
Strategy	**Strategy, Roadmap and Policy** • National Cybersecurity Policy – launched in 2014. • National ICT Policy. • Universal Access Policy – stipulates that at least 98% of the country should have connectivity. **Institutional Bodies** • Office of the Government Chief Information Officer (OGCIO) – leads cyber security. • Vanuatu CERT (launched circa June 2018). • Ministry of Justice – leads child exploitation prevention. • Vanuatu Police Force (VPF). • Telecommunications Radiocommunications and Broadcasting Regulator (TRBR) – managing CCTLD (.vu), recently transferred from Telecom Vanuatu. The TRBR are also involved in DNS security, associated training and child protection. **Training and Awareness** • Vanuatu CERT sends SMS messages twice a week to the entire country to provide awareness on cyber security. This was noted as very effective by multiple parties. • Cyber Safety Pasifika delivering cyber safety training and awareness in Vanuatu. • Constable Jeff Natapei from the VPF has hosted a radio program on Radio Vanuatu to deliver Cyber Safety Messages to the community. This has been a regular program and is well received in the community. • Vanuatu CERT has been completing (2019) a large awareness programme for communities, schools and local ISPs, and provides training to Vanuatu Police. • ITU has provided a number of 1 week training sessions on cyber security. • FireEye (a security monitoring vendor) have provided training through DFAT. • APNIC has provided cyber crime training. **Risk Management** • None identified to date.	• A National Cyber Security Strategy is in draft (led by Vanuatu CERT). • Working to establish a child online protection working group to identify areas for child online protection. • The Vanuatu CERT are proposing the "Vanuatu Research and Development Unit" who would focus on smart procurement of ICT and security products – confirming they are adequately supported and fit-for-purpose in terms of local requirements. In addition, they want to create more consistency in purchases across the region so skills can be shared. • The National Security Strategy (in draft) includes cyber security as a strategic concern.

Secure	**Legislation** The associated Chapman Tripp analysis outlines the following: • Cybercrime (substantive) – initial. • Cybercrime (child protection) – established. • Cybercrime (procedural) – initial. • Electronic transactions – established. • Privacy – initial. • Data protection – initial. • Digital authentication – none. • Consumer protection – initial. • Intellectual property – established. **Capability** • Vanuatu CERT includes three cyber security specialists with technical and governance capabilities. • TRBR has capability in regards to DNS security. • Pacific IGF has capability in regards to cyber policy and legislation. **Requirements and Standards** • Government websites are pages are being verified with a "blue tick" by CERT/OGCIO.	• Vanuatu is in the process of drafting a Cyber Bill, with substantive criminal law provisions to enable prosecution of cyber crimes such as illegal access, data interference, computer related fraud and cyber stalking. We understand a bill relating to the sending of spam emails is also in progress. Required changes to supporting legislation have been identified such as the Police Powers Act and Mutual Assistance in Criminal Matters Act. The goal is to have the new legislation align with the Budapest Convention. • Ministry of Justice are considering the need for privacy legislation.
Vigilant	**International Co-operation and Intel** • Member of the Pacific Island Law Officers' Network (PILON) • Member of Pacific Cyber Security Operational Network (PaCSON) • NZ CERT. • Australian Federal Police (AFP) – who have circa 12 liaison officers in Vanuatu to provide support and training (not only for cyber security). • INTERPOL – who have an office in Vanuatu. • The Council of Europe has provided in-country assistance with cyber legislation drafting. **Detection and Monitoring** • Vulnerability scanning and penetration testing is being performed from some organisations by Vanuatu CERT. • Local ISPs can provide logging information (i.e. txt and call records) when required by law.	• Currently formalising relationship with New Zealand Police and Australian Federal Police for cyber security assistance.

Resilient	**Connectivity and Redundancy**
	• Single submarine cable.
	• Multiple ISPs, including:
	  ○ Telecom Vanuatu Limited
	  ○ Digicel Vanuatu Limited
	  ○ Telsat Broadband Limited
	  ○ Wantok Network Limited
	
	Cyber Incident Response (CERT)
	• Vanuatu CERT have established a relationship with Facebook to assist in taking down inappropriate or fake pages.
	• Vanuatu CERT was established in 2018. It is funded by OGCIO and DFAT. The CERT includes three capable staff (technical and governance) and is administered by the OGCIO. The CERT is focused on:
	  ○ Providing advice to Government
	  ○ Establishing MOUs with other regional CERTs
	  ○ Developing/updating standards
	  ○ Penetration testing / vulnerability scanning
	  ○ Awareness and training
	
	Cyber Crime Enforcement
	• Incidents can be reported to the Crime Prevention Unit of the Vanuatu Police Force or to the Vanuatu CERT.
		• Working currently to establish a national CERT.
		• Working to establish a unit within law enforcement that serves as single point of contact for requests from government institutions as well as citizens and businesses

Previous Cyber Incidents	Based on our conversations with stakeholder representatives, we have captured a number of previous cyber incidents based on anecdotal evidence: • Recently there have been targeted phishing attacks against workers who are part of the New Zealand and Australia Recognised Seasonal Employer (RSE) schemes. These attackers are calling workers directly and have access to significant accurate information. They attempt to extract money from workers on behalf of the schemes. • Fraud cases where international actors have impersonated local or international businesses to entice local people to send money out of Vanuatu via Western Union. These have largely used email or Facebook Messenger as a medium to execute the attacks. • Child exploitation/pornography – an international person entered Vanuatu via boat, using gifts to entice young people from the outer islands onto their boat. Subsequently the children were abused and/or objective material was created. This person has been prosecuted using the penal code, but escaped custody. Their boat has been confiscated. • Facebook pages have been established which imitate key institutions such as the reserve bank and Government websites. • There have been a large number of complaints in regards to cyber bullying, revenge porn and online defamation. • Some DDoS attacks have been performed on Vanuatu / institutions based in Vanuatu, including against the core CCTLD registry (.vu). • A number of local and international banks operating in Vanuatu have been victims of card skimming and online account hacking. A number of prosecutions have been successfully achieved for both local and international attackers executing these attacks.	

Key Cyber Risks – Vanuatu



Research Sources

The following table is a summary of documents accessed during research and a list of Institutions and people, either spoken with over the phone or in country meetings. Each country has been given a rating to reflect the level of consultation:

- ■ Desktop only research.
- ■ ■ Desktop research and phone conversations.
- ■ ■ ■ Desktop research and in-country meetings.

Cook Islands	Level of Consultation ■ ■ ■	
Resource	**Author**	**Date**
Telecoms, mobile and Broadband - market Insights and statistics (14th Ed)	BuddeComm	August 2014
National Information and Communication Technology Policy 2015 - 2020	Government of the Cook Islands	July 2015
e-Government in the Pacific Island states: ICT policy and implementation in small island developing states (Cook Island Country Report)	Rowena Cullen and Graham Hassall	2016
Government of the Cook Islands Internet Usage Policy	Government of the Cook Islands	
ICT Office, Office of the Prime Minister Report	Kenrick Fernandes and Tepua Hunter	August 2012
National Sustainable Development Plan 2016 – 2020	Government of the Cook Islands	January 2016
Cook Islands balancing geopolitical relationships	Dateline Pacific (RadioNZ)	April 2018
Questions over number of MPs as Cook Island election approaches	RadioNZ	May 2018
Cook Islands ICT Facebook page	Facebook.com	
Map - List of ISP in Cook Islands	Allisps.com	2018
Map - Internet Providers in Cook Islands	Satproviders.com	2018
Telecommunications in the Cook Islands	Wikipedia	July 2018
O3b Networks	Wikipedia	June 2018
Cook Islands	Wikipedia	July 2018
Cybercrime policies/strategies	Council of Europe	January 2018
Institutions/Interviewees		**Date**
Ministry of Finance		April 2018

Crown Law Office		April 2018
Cook Island Police		April 2018
Cooks Islands main telecom providers		April 2018
Critical infrastructure providers – power, water		April 2018

Fiji	Level of Consultation ■ ■ ■	
Resource	**Author**	**Date**
Telecoms, mobile and broadband statistics and analyses (19th Ed)	BuddeComm	June 2017
Telecoms, mobile and broadband statistics and analyses (20th Ed)	BuddeComm	June 2018
Cybersecurity in the Republic of Fiji	Salanieta Tamanikaiwaimaro	July 2016
Cybersecurity Situation In Fiji	Shelveen Pandey, Nadeem Shah, Amit Sharma, Mohammed Farik	July 2016
Fiji Profile	International Telecommunication Union	2017
Fiji Cyber Wellness Profile	International Telecommunication Union	August 2014
Fiji Country Report	Economist Intelligence Unit	February 2018
Institutions/Interviewees		**Date**
Ministry of Defence and National Security		March 2019
University of the South Pacific / CROP ICT Working Group		March 2019
Fiji Police		March 2019
Ministry of Communications		March 2019
Office of the Attorney General		March 2019
Office of the Auditor General		March 2019
Reserve Bank of Fiji		March 2019
Pacific Forum Secretariat		March 2019

Federated States of Micronesia (FSM)	Level of Consultation ■ ■	
Resource	**Author**	**Date**

Telecoms, mobile and broadband – statistics and analyses (3rd Ed)	BuddeComm	August 2016
Federated States of Micronesia	Wikipedia	July 2018
Micronesia Profile	International Telecommunication Union	2017
Marine Division - Regulations	Department of Transportation, Communications & Infrastructure	2017
FSS Unity officially joins FSM Maritime Surveillance fleet	Government of the Federated States of Micronesia	August 2012
Maritime interdiction (Agreement between U.S.A. and Micronesia	U.S. Department of State	May 2008
ADB approves US$36m for internet in Micronesia	RadioNZ	April 2018
Telecommunications in the Federated States of Micronesia	Wikipedia	June 2018
Cyber Wellness Profile Micronesia (Federal States of)	International Telecommunication Union	August 2014
The Federated States of Micronesia National ICT and Telecommunications Policy	Government of the Federated States of Micronesia	September 2012
Overview of ITU activities on Cybersecurity	International Telecommunication Union	March 2014
The World Factbook - Micronesia, Federated States of	Central Intelligence Agency (US)	
Map - List of ISP in Micronesia	Allisps.com	2018
Cybercrime policies/strategies	Council of Europe	January 2018
Federated States of Micronesia country brief	Department of Foreign Affairs and Trade (Australia)	
Foreign relations of the Federated States of Micronesia	Wikipedia	May 2018
Economy of the Federated States of Micronesia	Wikipedia	May 2017
U.S. Relations With the Federated States of Micronesia	U.S. Department of State	October 2017
Micronesia country profile	BBC News	January 2018
America's Micronesia Problem	Thomas R. Matelski	February 2016
Institutions/Interviewees		**Date**
Brensen B. Penias - National Police, Lieutenant/Investigator		June 2018
Bia Nanoto - National Police, Captain		June 2018
Kasner Alden - National Police, Lieutenant/Investigator		June 2018

Kiribati	**Level of Consultation** ■ ■	
Resource	**Author**	**Date**

Kiribati Profile	International Telecommunication Union	2017
Kiribati Cyber Wellness Profile	International Telecommunication Union	August 2014
Telecoms, Mobile and Broadband Statistics and Analyses (14th Ed)	BuddeComm	July 2016
Institutions/Interviewees		**Date**
Taaira Timeon - State Attorney, Office of the Attorney General		June 2018
Waimauri Nawaia - State Attorney, Office of the Attorney General		June 2018
Akau Matirei Terite - Police Officer, Kiribati Police Service and Prisons		June 2018

Marshall Islands	**Level of Consultation** ■ ■ ■	
Resource	**Author**	**Date**
Australian Country Report 2017	Attorney-General's Department (Australia)	October 2017
Telecoms, Mobile and Broadband – Statistics and Analyses (3rd Ed)	BuddeComm	August 2016
National Strategic Plan 2015–2017	Economic Policy, Planning and Statistics Office of the Marshall Islands	June 2014
Marshall Islands	Wikipedia	July 2018
Marshall Islands Profile	International Telecommunication Union	2017
Cyberwellness Profile Marshall Islands	International Telecommunication Union	August 2014
EU set to remove Bahrain, Marshall Islands, Saint Lucia from tax haven list	Reuters	March 2018
Marshall Islands e-mail service disrupted by cyber attack	RadioNZ	June 2008
Marshalls internet still affected after cyber attack	RadioNZ	June 2008
Report of Independent Auditors and Financial Statements	Marshall Islands National Telecommunications Authority	September 2012
Marshall Islands National Telecommunications Authority Contributes to Responsive and Resilient Internet with L-Root Instance in Marshall Islands	ICANN	March 2017
Meet the 'Sovereign': Marshall Islands Government to Issue Crypto Token	Annaliese Milano	February 2018
Tired of Waiting for the Internet Repairman? Just Be Glad You're Not in the Marshall Islands	Feliz Solomon	January 2017
Communications in the Marshall Islands	Wikipedia	June 2016

The World Factbook – Marshall Islands	Central Intelligence Agency (US)	
Marshall Islands Police Department	Facebook.com	
Marshall Islands	U.S. Department of State	March 2003
Law enforcement in the Marshall Islands	Wikipedia	December 2017
PacCERT	Facebook.com	
Institutions/Interviewees		**Date**
Dr.Falai Riva Taafaki - Chief Prosecutor / Office of the Attorney General		June 2018 / July 2019
Jaston Anjain – Digital Forensics / Auditor, Office of Auditor General		June 2018 / July 2019
Marshall Islands Social Security Administration (MISSA)		July 2019
Banking Commissioners Office		July 2019
Ministry of Foreign Affairs		July 2019
RMI Police		July 2019
RMI National Telecommunications Authority (NTA)		July 2019
Critical Infrastructure Provider (power)		July 2019
Critical Infrastructure Provider (water)		July 2019
Ministry of Finance		July 2019
Ministry of Education		July 2019
RMI University of the South Pacific (USP)		July 2019

Nauru	**Level of Consultation** ■	
Resource	**Author**	**Date**
Nauru Cyber Wellness Profile	International Telecommunication Union	August 2014
The Republic of Nauru Technology Updates	Joel Waqa	2016
Nauru Profile	International Telecommunication Union	2017
Nauru - Telecoms Market Overview & Statistics	BuddeComm	January 2010
Nauru	Wikipedia	July 2018
NAURU 2017/2018	Amnesty International	
Crime in Nauru	Wikipedia	September 2017

Telecommunications in Nauru	Wikipedia	December 2017
Utilities of Nauru	Nexus Commonwealth Governance	2018
Find Telecommunication expertise in Nauru	Nexus Commonwealth Network	2018
The Republic of Nauru's ISP since 1998	CenpacNet Inc.	
Telecommunications and Regulatory Affairs (Amendment) Act 2017	Republic of Nauru	May 2017
Telecommunications and Regulatory Affairs Act 2017	Republic of Nauru	May 2017
Cybercrime policies/strategies	Council of Europe	January 2018
Nauru police raids on Save the Children sparked by detention centre's manager	The Guardian	October 2015
Nauru complaint triggers charity raid	RadioNZ	October 2015
The World Factbook – Nauru	Central Intelligence Agency (US)	August 2008
Nauru struck off tax haven blacklist	ABC News	December 2003
Overview of Australia's aid program to Nauru	Department of Foreign Affairs and Trade (Australia)	
Foreign relations of Nauru	Wikipedia	July 2018
Economy of Nauru	Wikipedia	June 2018

Niue	**Level of Consultation** ■ ■	
Resource	**Author**	**Date**
Telecoms, Mobile and Broadband - Market Insights and Statistics (13th Ed)	BuddeComm	August 2014
Niue Island Overview	Niue Island Government	2017
Cybercrime policies/strategies	Council of Europe	
Pilot programme regarding cyber crime targets Niue students	RadioNZ	August 2008
Institutions/Interviewees		**Date**
Aldric Nicko Tulipo T. Hipa - Assistant Crown Counsel		June 2018
Narita Janne Freda T. Tahega - Constable, Niue Police		June 2018
Helemaiheiki Hender T. Poumale - Head Data and Information Agency		June 2018

Palau	**Level of Consultation** ■ ■

Resource	Author	Date
Republic of Palau Cyber Wellness Profile	International Telecommunication Union	March 2015
Palau Criminal Procedure	Republic of Palau	
Telecoms, Mobile and Broadband – Statistics and Analyses (15th Ed)	BuddeComm	May 2017
Telecommunications Regulatory Framework	Republic of Palau	May 2017
Institutions/Interviewees		**Date**
Lebuu Gibbons - Detective Lieutenant, Criminal Investig. Div, MOJ		June 2018
Virginia Umayam - Investigator, Office of the Attorney General		June 2018
Dolyn Tell - Criminal Investigator, Office of the Attorney General		June 2018

Papua New Guinea (PNG)	Level of Consultation ■ ■	
Resource	**Author**	**Date**
Papua New Guinea Country Report	Economist Intelligence Unit	February 2018
Papua New Guinea Cyber Wellness Profile	International Telecommunication Union	August 2014
Papua New Guinea Profile	International Telecommunication Union	2017
Papua New Guinea Cybercrime Policy	National Parliament of Papua New Guinea	December 2016
Cybercrime Code Act 2016	National Parliament of Papua New Guinea	December 2016
Telecoms, Mobile and Broadband – Statistics and Analyses (19th Ed)	BuddeComm	January 2018
Institutions/Interviewees		**Date**
Josephine Pitmur - Director, Legal Policy and Governance Branch		June 2018
Jemimah Taru - Senior Legal Privacy Officer, DOJ and Attorney General		June 2018
Serah Osembo - Legal Officer, Public Prosecutors Office		June 2018

Samoa	Level of Consultation ■ ■ ■	
Resource	**Author**	**Date**
Samoa Country Report	Economist Intelligence Unit	February 2018
Samoa Profile	International Telecommunication Union	2017

Samoa Cyber Wellness Profile	International Telecommunication Union	September 2014
Samoa National Cybersecurity Strategy 2016 – 2021	Government of Samoa	2016
Government Internet and E-mail Policy 2016	Government of Samoa	2016
Work For $5m Submarine Cable Depot Begins	Ivamere Nataro	March 2018
e-Government in the Pacific Island states: ICT policy and implementation in small island developing states – Samoa Country report	Rowena Cullen, Ioana Chan Mow, and Graham Hassall	2016
Telecoms, Mobile and Broadband – Statistics and Analyses (15th Ed)	BuddeComm	July 2016
Cybersecurity Capacity Review (Independent State of Samoa)	University of Oxford (https://mcit.gov.ws/wp-content/uploads/2019/04/20190402-CMM-Samoa-Report.pdf)	December 2018
Institutions/Interviewees		**Date**
Ministry of Finance		May 2018
Attorney General's Office		May 2018
Samoa Police		May 2018
Samoa main telecom providers		May 2018
Critical infrastructure providers – power, water		May 2018
National Reserve Bank		May 2018

Solomon Islands	**Level of Consultation** ■ ■ ■	
Resource	**Author**	**Date**
Telecoms, Mobile and Broadband – Statistics and Analyses (14th Ed)	BuddeComm	September 2016
Solomon Islands Profile	International Telecommunication Union	2017
e-Government in the Pacific Island states: ICT policy and implementation in small island developing states – Solomon Islands Country report	Rowena Cullen and Graham Hassall	2016
Solomon Islands Country Report	Economist Intelligence Unit	February 2018
Solomon Islands Cyber Wellness Profile	International Telecommunication Union	January 2015
Institutions/Interviewees		**Date**
Mr. Felix Hollison, Senior Crown Counsel, Attorney General's Chambers		June 2018
Central Bank of Solomon Islands (CBSI)		June 2018

Telecommunications Commissions of Solomon Islands (TCSI)	June 2018
Director of Public Prosecutions (DPP)	June 2018
Critical infrastructure providers – power, water, gas (Solomon Power and Solomon Water)	June 2018
Telecommunication Commission of Solomon Islands and Telecommunication and Internet Service Providers (ISPs)	June 2018
Technical lead for Government ICT/tech	June 2018
Attorney General's Chambers	June 2018
Office of the Director of Public Prosecutions	June 2018
Law Reform Commission	June 2018
MJLA's Legal Policy Unit	June 2018
Ministry of Communication and Aviation	June 2018
Ministry of Finance and Treasury and S.I.G Information & Communication	June 2018
Royal Solomon Islands Police Force (RSIPF)/Transnational Crimes Unit (TCU)	June 2018
Central Bank of Solomon Islands (CBSI)	June 2018

Tonga	**Level of Consultation** ■ ■ ■	
Resource	**Author**	**Date**
Tonga Country Report	Economist Intelligence Unit	February 2018
Tonga Cyber Wellness Profile	International Telecommunication Union	August 2014
Tonga Profile	International Telecommunication Union	2017
Telecoms, Mobile and Broadband – Statistics and Analyses (3rd Ed)	BuddeComm	September 2016
Forum Compact Peer Review Report – Kingdom of Tonga	Pacific Islands Forum Secretariat	October 2012
Tonga	Wikipedia	July 2018
Human rights in Tonga	Wikipedia	June 2018
Telecommunications in Tonga	Wikipedia	December 2015
PM launched Tonga National CERT	Ministry of Information and Communications	July 2016
Tonga CERT study trip comes to APNIC	Adli Wahid	April 2017

Phishing Fraud Occurred Again This Week	Radio & TV Tonga	July 2017
Government Structure and ICT People (Google Groups)	tg-egov	December 2017
National Reserve Bank of Tonga	Wikipedia	February 2018
Government wants Reserve Bank to 'run a tight ship'	Matangi Tonga Online	March 2018
Tonga Cable Limited Website	Tonga Cable Limited	2018
Tonga Cable System	Wikipedia	July 2018
The Tonga Energy Sector Legal Framework: How legislation will assist the role of the Regulator	Sela Bloomfield	August 2016
Mr. Paula Pouvalu Ma'u, appointed Commissioner for ASTANA EXPO-2017 Kazakhstan	Ministry of Information and Communications	March 2017
Tongan Legislation website	Attorney General's Office, Tonga	2018
Attorney General's Office – Tonga	Facebook.com	
Denis O'Brien's Digicel pays €3.6m for Tonga Cable stake	Barry O'Halloran	July 2017
Digicel	Wikipedia	July 2018
Attorney General (Tonga)	Wikipedia	July 2018
Move to sack Tongan police chief lays bare 'prohibited' guns imports	Kaniva News	March 2018
Computer Crimes Act, 2003	World Intellectual Property Organization	September 2003
Tonga conducts Cybersecurity and Cybercrime workshops	Ministry of Information and Communications	March 2013
Tonga and ADB	Asian Development Bank	2018
Tonga National CERT Signs a Framework of Operational Cooperation (FOC) with the CERT Australia to manage Cyber Security	Ministry of Information and Communications	May 2018
Tonga-Australia Sign Agreement To Share Cyber Security Information	Pacific Islands Report	May 2017
Gov't of Tonga & Waikato to collaborate on cyber security	University of Waikato	May 2017
How a Waikato Uni grad transformed Tonga's cyber security	Sara Barker	June 2017
Waikato Uni & Tongan Government stand side by side for cyber security	Sara Barker	May 2017
Waikato Uni student presents cybersecurity research to Tongan IT experts	Sara Barker	February 2017
Vital to Minimize Cyber-crimes in Tonga and the Region	Radio & TV Tonga,	May 2017
Tonga joins the Budapest Convention on Cybercrime	Ministry of Information and Communications	May 2017
Sovaleni Points to Cybercrime Challenges	Nuku'alofa Times	May 2017
Institutions/Interviewees		**Date**

Mr. Paula Ma'u, CEO MEIDECC	April 2018
Tonga CERT Board members	April 2018
Daniel Henson, BSP Bank	April 2018
Sulia Toutai, Manager Compliance, ANZ Bank	April 2018
Maikolo Pifeleti, Manager IT, ANZ Bank	April 2018
Kasaline Lolohea, Corporate Services, NRBT	April 2018
Dennis Fuapau, Head of Business Solutions, Digicel Ltd	April 2018
Ragigia Dawai, Head of Consumer Sales, Digicel Ltd	April 2018
Mr. Áminiasi Kefu, Acting Attorney General and Public Prosecutor	April 2018
Inoke Finau, Assistant Crown Counsel	April 2018
Leotrina Macomber, Assistant Crown Counsel	April 2018
Police Commissioner Steven Caldwell	April 2018
A/Deputy Commissioner Kalisi Tohifolau	April 2018
Siumafua Moala, Tonga Cable	April 2018
Lualala Tapueluelu, Tonga Power Ltd	April 2018
Karl Sanft, Tonga Water Board	April 2018
Ms. Jessie Cocker, Deputy Governor, NRBT	April 2018
Kasaline Lolohea, Senior Manager - Corporate Services, NRBT	April 2018

Tuvalu	**Level of Consultation** ■ ■	
Resource	**Author**	**Date**
Tuvalu Cyber Wellness Profile	International Telecommunication Union	August 2014
Tuvalu Profile	International Telecommunication Union	2017
Project Information Document/Integrated Safeguards Data Sheet (PID/ISDS)	The World Bank	November 2016
Telecoms, Mobile and Broadband – Statistics and Analyses (3rd Ed)	BuddeComm	September 2016
Investment & Internet Connectivity in Tuvalu	UN Office of the High Representative for the Least Developed Countries	2017
Government of Tuvalu 2017 National Budget	Government of Tuvalu	November 2016

Country Operations Business Plan: Tuvalu, 2017–2019	Asian Development Bank	October 2016
Tuvalu country profile	BBC News	February 2018
Institutions/Interviewees		**Date**
Efren Jagdish Jogia - Senior Crown Counsel, Office of the AG		June 2018
Iuni Soloseni - Police Inspector, Tuvalu Police Office of PM		June 2018
Iunipa Siaeki - Senior ISP Officer, MCTICT Dept		June 2018

Vanuatu	**Level of Consultation** ■ ■ ■	
Resource	**Author**	**Date**
Vanuatu Country	Economist Intelligence Unit	February 2018
Vanuatu Profile	International Telecommunication Union	2017
Cybersecurity: Policy Development and Challenges for Vanuatu	Lloyd M. Fikiasi	December 2013
e-Government in the Pacific Island states: ICT policy and implementation in small island developing states – Vanuatu Country report	Rowena Cullen and Graham Hassall	2016
Child Online Protection. Assessment, Challenges, Opportunities and Way Forward for Vanuatu	Ronald Box	September 2014
Telecoms, Mobile and Broadband – Statistics and Analyses (16th Ed)	BuddeComm	July 2016
Institutions/Interviewees		**Date**
Philip Toaliu - State Prosecutor, Office of Prosecutor		June 2018
Louise Nasak - HR Adviser, Cybercrime Policy Coordinator, MOJ		June 2018
Jimmy Nimisa John - Police Constable, Family Protection Unit		June 2018
CERT Vanuatu		July 2019
Office of the Telecommunications and Radio-communications Regulator (TRBR)		July 2019
Office of the Government Chief Information Officer		July 2019
Office of the Public Prosecutor		July 2019
Vanuatu Police		July 2019
Chamber of Commerce		July 2019
Vanuatu IGF		July 2019

Pacific Group Ltd	July 2019
BRED Bank Vanuatu	July 2019

General

Resource	Author	Date
Pacific Islands Law Officers' Network cybercrime Workshop 23 – 25 May 2017, Nuku'alofa, Kingdom of Tonga	Ministry of Information and Communications	May 2017
Mooney Laundering and Financial Crimes Country Database	U.S. Department of State	May 2012
GLACY+: Pacific Islands Law Officers' Network Cybercrime Workshop	Council of Europe	May 2017
Cyber Safe Pasifika	Global Cyber Security Capacity Centre	December 2017
Submarine Cable Map	submarinecablemap.com	2018
Australia tackles regional cyber resilience	Justin Hendry	October 2017
The Mobile Economy Asia Pacific 2017	GSMA Intelligence	2017
GSMA Ecosystem Accelerator Innovation Fund	GSMA Intelligence	2017
Pacific Islands CERT (PacCERT) - Updates & Current Status	The University of the South Pacific	June 2015
Intelsat	Wikipedia	February 2018
Pacific to establish cybercrime collaborative platform as threat escalates	The Commonwealth	February 2016
Pacific cybercrime network hailed by small island states	The Commonwealth	March 2016
Capacity Building and ICT Policy, Regulatory and Legislative Frameworks Support for Pacific Island Countries (ICB4PAC)	International Telecommunication Union	November 2009
Cyber Maturity in the Asia-Pacific Region	International Cyber Policy Centre	2016
Asia-Pacific Cybersecurity Dashboard – A Path to a Secure Global Cyberspace	BSA, The Software Alliance	2015
New Zealand's Cyber Security Strategy – Action Plan	New Zealand Government	2015
New Zealand's Cyber Security Strategy – Action Plan Annual Report	New Zealand Government	2016
Cyber Risk in Asia-Pacific – The Case for Greater Transparency	Marsh & McLennan Companies	2017
Cyber Security and Legislation in the Pacific	A H Angelo	2008
Cyber Regulations in Asia Pacific	Deloitte	2017

Cybercrime Legislation Amendment Act 2012	Australian Government	
Cyber Maturity in the Asia-Pacific Region	International Cyber Policy Centre	2016

Part B

Cybersecurity and Safeguarding Electronic Transactions in the Pacific Islands

Policy and Legal Gap Analysis

Contents Part B

Executive Summary

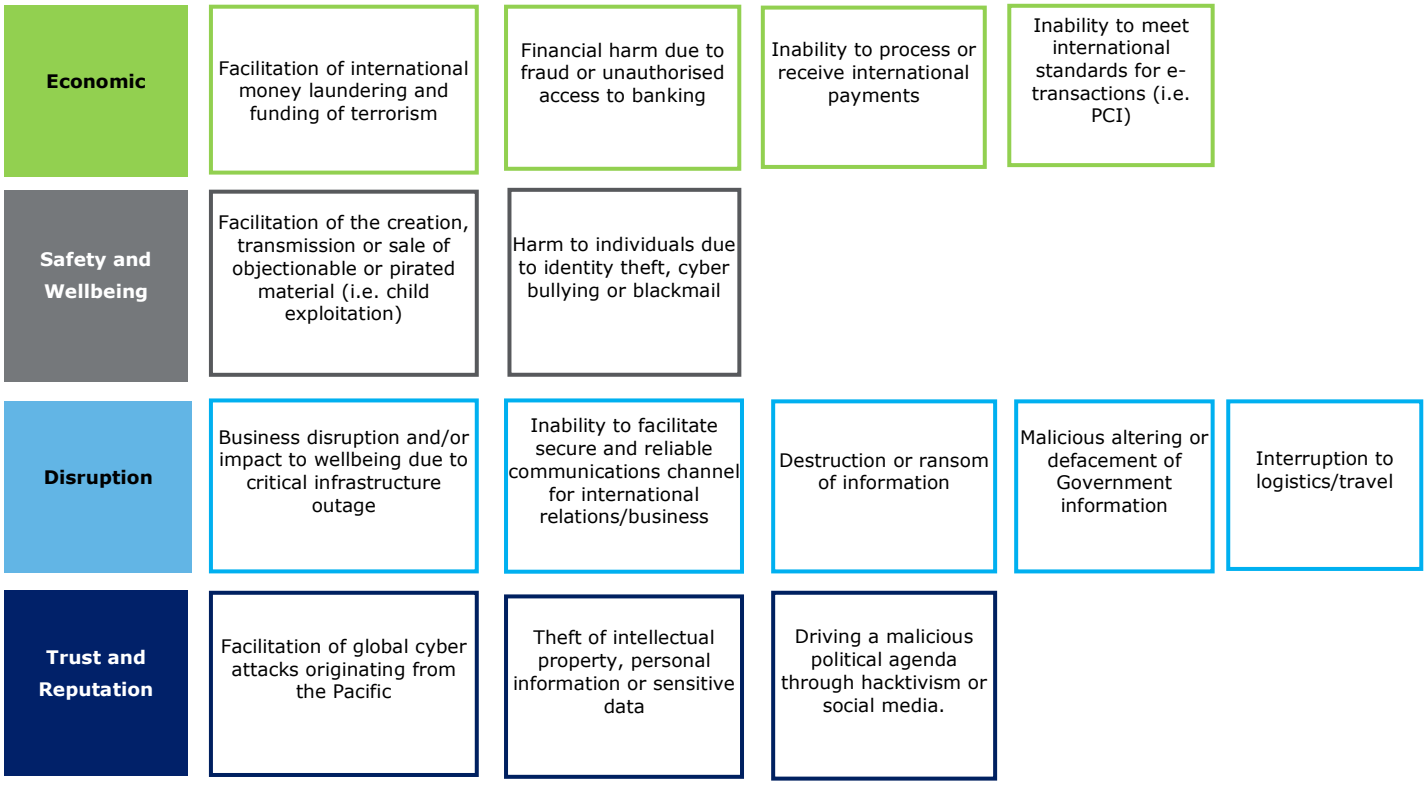
Key regional insights

TIMING

The Pacific region is exposed to the cyber threats that the rest of the world is grappling with - from cyber bullying and card skimming to phishing and false invoices to child pornography. This has not only caused financial losses running to millions of dollars, presenting a very real threat to financial systems in the region, but also a risk of harming the physical and mental wellbeing of the region's citizens.

The risk footprint will become larger as Pacific countries increase their online connectivity through improved infrastructure, increased uptake of social media, improved ICT literacy and increased availability of, and reliance on, e-services. Now is the time for governments to take measures to address cybersecurity issues effectively, such as through greater awareness, capacity building and improved legal and regulatory frameworks.

Deloitte has identified 14 key types of cyber risks that the Pacific region currently faces across 4 harm areas:



These localised risks can have global consequences, creating a global responsibility to have appropriate cybersecurity, vigilance and resilience in the region.

We note that some countries in the Pacific have relatively limited connectivity and low and/or scattered populations, and lower value at risk compared to global targets. Those practical constraints mean cyber risks are currently somewhat nascent. However with limited awareness and reporting also, it is hard to be definitive about the current level of activity. Our in-country consultations identified that in more developed Pacific countries like Vanuatu, Samoa and Tonga, cyber risks have come to pass.

Looking forward, the continuing drive to connect the Pacific by submarine cable and satellite means that all Pacific countries will be increasingly vulnerable to these risks. The expected increase in online shopping / transactions and payments, use of social media, and digital control systems for important infrastructure, are also relevant. The time for Governments to take action is now. The purpose of this report is to help prioritise attention and funding to those areas which will make the most difference in raising the standard in all Pacific countries on cyber issues.

IMPORTANCE OF FRAMEWORKS

There is the opportunity for the Pacific to make a good amount of progress in a relatively short period of time.

In our discussions Pacific stakeholders regularly emphasised the importance of getting legal and regulatory frameworks in place, as a way of guiding policy focus and capacity building. While in the cybersecurity area a lot of Pacific countries are starting from a low base, the fundamental building blocks that are needed are well known, and highlighted in this report. The task for each jurisdiction over the next couple of years is to get the fundamental building blocks in place.

Some Pacific countries have developed cybersecurity strategy documents (for example, Papua New Guinea, Samoa and Vanuatu). These are valuable as they establish a common picture for the public and private sector in each country about the priority actions on cybersecurity over the next couple of years. All of the Pacific stakeholders we spoke to supported the view that each country would benefit from a strategy document that captures the national story on cybersecurity.

Other big gains to be made include:

- Each country clearly establishing how it will manage cybersecurity for critical infrastructure and systems (including government information systems);
- A number of Pacific countries have enacted criminal law legislation for cyber-crime offences modelled on the Budapest Convention, or are in the process of upgrading existing law to this standard. Pacific countries can continue this effort, and learn from experiences to date as they do so;
- This legislative progress can and should be supported by a focus on building the capacity for effective investigation, enforcement, prosecution and adjudication of offences. Across most of the Pacific, building the front-line capacity for responding to cybercrime is a major opportunity for improving cyber-security.
- We particularly want to emphasise how this investment in effective investigation, enforcement, prosecution and adjudication can address the risks of cyber bullying and [child exploitation]. These issues were stressed to us during consultations as being current and serious risks, with consequences for individuals and communities.

As well as these frameworks, our gaps analysis, risk assessment, and discussions with Pacific stakeholders to date indicate that Pacific governments can improve the management or mitigation of cybersecurity risks by investing in:

- capacity (regulatory, enforcement, technical);
- public awareness of the size, scope and scale of risk, and the roles that all individuals can play in reducing these risks;
- a consistent regional approach to identifying, reporting and sharing information on cyber risks, cyber incidents, and practical mitigations across the region.

OPPORTUNITY TO ADDRESS RISKS AT REGIONAL LEVEL

In our view, we see the key regional opportunities as being:

- implementing cybersecurity and digital strategy in the region and developing a consistent approach to coordinating strategy across the Pacific, where interconnectedness requires a coordinated and consistent approach;
- preparing a legal framework which sets out key functions and responsibilities of cyber stakeholders, deals with cybercrime, and allocates funding;
- building capacity at a regulatory, enforcement and technical level and identifying a clear strategy or funding to develop regional resource and capacity;
- improving cybersecurity safeguards for critical infrastructure; and
- increasing public awareness of cybersecurity and digital issues.

In these areas there is the opportunity for governments and development partners to aim for consistency of approach and implementation across the region. This will help with the development of common knowledge and expertise across the Pacific, as well as promote efficiencies in implementation.

Our recommendations address each of these opportunities for improvement.

Regional Recommendations

Although the countries considered in this study are in varying states of legislative and regulatory development for cybersecurity and electronic transactions, we have identified a number of consistent trends across the Pacific region. These trends enable us to make the following recommendations for regional-level development.

We have also recommended a prioritisation of effort. While all of the proposals discussed in this report will improve circumstances in the Pacific, they cannot all be done at once.

An effective reform can involve building the understanding and demand for change, introducing quality and appropriate legal frameworks, and, most importantly, investing over several years in the institutions charged with implementation. Done well, each reform will involve a lot of effort. Pacific jurisdictions, like all jurisdictions, must prioritise their efforts.

When thinking about prioritisation in this area, Governments and development partners will weigh up the scale and capacity of existing institutions in-country, the capacity for reform and implementation of new laws and enforcement of those laws, the current state of progress in-country on cybersecurity, and the current level of online commercial activity and whether supporting legislation is needed at this stage.

It is important, too, to bear in mind that scale varies significantly across the Pacific. Using population as a rough estimate of scale, the variation in scale across this study is as follows:

Country	Population
Papua New Guinea	8,418,300
Fiji	912,241
Solomon Islands	623,300
Vanuatu	282,100
Samoa	197,700
Kiribati	118,400
Kingdom of Tonga	109,000

Federated States of Micronesia	106,200
Republic of the Marshall Islands	53,100
Palau	22,000
Cook Islands	17,400
Nauru	11,300
Tuvalu	11,300
Niue	1,600

We consider some urgency should be attached to implementing, in a way appropriate for local scale and circumstances, recommendations 1 to 5 below (priority I recommendations). As a generalisation, and depending on the circumstances in each country, the cybersecurity building blocks should be prioritised over the commercial law frameworks. At a basic level, developing cybersecurity strategies, capacity and awareness building and safeguarding critical infrastructure across the region are high priority needs, to ensure Pacific countries are not left vulnerable as the region becomes more connected, digitally focussed and, consequently, a potential target for hackers and fraudulent digital operators. Recommendations 6 to 9 can be considered priority II recommendations. As we identify in the individual country recommendations, some of the larger Pacific countries that are more advanced with their cybersecurity initiatives are better placed, and have more of a need, to give the commercial frameworks some priority.

Priority I recommendations

1 Develop cybersecurity strategies

Coordinated action to address cybersecurity risk at a country level starts with a documented cybersecurity strategy. Countries with a well-prepared strategy or cyber policy include Papua New Guinea, Samoa and Vanuatu. Developing a cybersecurity strategy is an important step to identify and prioritise goals, determine institutional responsibility and allocate resources. A strategy will give impetus and direction to each country's efforts to improve its cybersecurity, especially if each strategy is updated every few years, so that it remains current.

We suggest there is value in developing a model or template cybersecurity strategy for Pacific countries to use as a starting point. Each country can then use the template to document the actions they intend to take to manage cyber risk. Some steps in this direction have already been taken: a close study of national ICT policies across the region was part of the ICB4PAC project, and the CTO prepared a "Commonwealth approach" for developing national cybersecurity strategies in 2015. Drawing this work together to develop an easy-to-use template would assist individual Pacific countries in the process of preparing their own cybersecurity strategies.

At the September 2018 Pacific Islands Forum, leaders endorsed the BOE Declaration on regional security, which expanded the concept of regional security to include, among other concepts, transnational crime and cybersecurity "to maximise protections and opportunities for Pacific infrastructure and peoples in the digital age". This helpfully elevated the profile and priority of cybersecurity in the region.

In response, the Pacific Islands Forum Secretariat has developed a draft action plan for implementation of the BOE Declaration by Pacific countries. Consultations on the draft action plan were held earlier this year. In relation to cybersecurity, the draft action plan proposes:

- promoting and supporting Forum Members accession to the Budapest Convention;
- sharing information on cybersecurity and cybercrime threats and trends;
- supporting the development of national cyber policies and legislation;
- promoting awareness and educating our people on responsible cyber behaviour; and,

- development and strengthening of Computer Emergency Response Team (CERT) capacities (national and regional).

This action plan helpfully maps against some of the priorities that were emphasised to us by Pacific stakeholders during our consultations, and key areas we would hope to see in a national cyber-security strategy.

We also understand that a Cybersecurity Centralised Monitoring initiative is proposed, through PIRRC. We recommend that the initiative include reporting mechanisms and processes to report regularly to identified stakeholders in each country on status and trends in cybersecurity (regionally, and globally), to help inform decision makers in each country when defining and implementing cybersecurity strategies.

2 Cybersecurity awareness

In practice the level of security in the Pacific can be lifted with a concerted effort on awareness, and basic training in cybersecurity hygiene.

Pacific leaders, policy makers, enforcement officers, government officials, financial institutions, infrastructure providers and the general public must understand the nature of the threats online so that they can protect themselves, and take the appropriate action when a threat arises. At the start, raising general awareness could be as simple and as cost effective as a short TV programme.

People regularly use the same email account for personal and work use. And yet individuals do not often receive the benefit of training on how to spot phishing and other cyber hacks that happen at the individual level. A lift in cyber-security hygiene can be the most effective measure in any company, institution or country.

We don't under-estimate the practicalities of rolling out training in the Pacific. Many Pacific countries are spread across a wide geographic area and achieving consistent and broad coverage of cyber awareness programmes can be challenging. There are helpful on-line tools that can be used, and various ways could be used to reach people: schools, the public sector, key infrastructure providers, and so on.

While Programmes like Cyber Safety Pasifika are doing a good job at raising awareness in many Pacific countries. While Cyber Safety Pasifika has been well received, stakeholders also recognised that it relies on the train-the-trainer model (in this case, the Police), which in turn relies on the local trainers having the capability, time and resources to deliver training in-country. Our in-country consultations identified a desire for more broad-based and coordinated awareness building.

Coordinated funding for public awareness building programmes at a regional level, with implementation at a local level, would be a useful regional initiative. A framework awareness building programme could be developed with cultural-specific implementation at a country level. That framework should cover programmes in schools, and community initiatives specifically addressing cyber bullying, child exploitation, as well as a broader programme of digital awareness for online transactions and fraud protection.

We are aware that USP and AFP are currently developing free cybersecurity awareness raising courses to be delivered online and offline. This is a promising development. When it comes to delivery we would encourage a focus on practical delivery channels in each country (for example, in Vanuatu, reminders are texted to all customers on mobile networks) and co-ordination with other efforts in the Pacific.

3 Continue to enact up-to-date cybercrime legislation

There is progress across the Pacific in enacting cybercrime legislation. A number of countries in the Pacific have either enacted cybercrime legislation modelled on the Budapest Convention or have processes underway to develop existing legislation to this standard. It is important that this effort continues, and that countries without modern cybercrime legislation are encouraged to reform their legislation as appropriate.

Many stakeholders we have spoken to confirmed that legislation drives changes in institutional behaviour around cybersecurity. Without legislation as a guideline to action, government agencies and other organisations find it hard to take it upon themselves to address cybersecurity and cybercrime issues. Furthermore, by formalising cybersecurity functions of key government ministries, these ministries should receive the budget support required to implement or enforce cybersecurity and cybercrime measures.

To date there have been a number of prosecutions for cyber-related crimes in the Pacific using local crime and penal code provisions. This has been a useful way to address cyber risks in the short term, but is considered by stakeholders to highlight the genuine need for up to date legislation.

The legislative drafting programmes run by the Australian Attorney-General's Office appear to have been particularly helpful in assisting countries to develop cybercrime legislation. We recommend expanding these programmes and/or funding similar exercises elsewhere, such as in the Northern Pacific. Some key benefits of this programme have been to create connections between different countries, as well as to facilitate thinking around governance, capacity and enforcement issues in-country while legislation is being developed. This programme, or a similar programme, could also create a channel for exchange of legislation drafting, helping countries at different stages of the legislation drafting process where capacity may be lacking or constrained. Alternatively, a model legislation template would assist individual Pacific countries to prepare their own cybercrime legislation. However, this option would still require the assistance of experienced legislative drafters – as enacting cybercrime legislation would require review of a number of existing laws, including laws relating to evidence, police, criminal offences, electronic transactions, consumer protection and financial institutions.

We also recommend that when updating cybercrime legislation, governments put in place enforcement protocols or memoranda of understanding between key enforcement stakeholders, such as the Attorney-General's office, Director of Public Prosecutions, Police, ISPs etc. Our consultations in-country confirm that stakeholders will benefit from having a formal framework to establish cooperation in enforcement, and to provide protocols to be followed by different stakeholders in response to a cybersecurity incident.

4 Capacity-building: law enforcement, prosecution services, law practitioners and the judiciary

A country's ability to enforce a cybercrime legislative framework relies on effective investigation, prosecution and adjudication of cybercrime offences. The effort of passing new laws is only worth it if there is also the follow up commitment to support the people and institutions who will be tasked with implementing the new laws.

In most Pacific countries, improving the capacity for responding to cybercrime is a high priority and a real opportunity to make gains. Significant effort should be devoted to improving this capacity, by providing training on investigating cybercrime and collecting digital evidence, and by ensuring appropriate resources (both human and financial) are allocated to combatting cybercrime. It may be most effective to conduct much of this training at a regional level, utilising instructors available from Australia, New Zealand and the United States.

As noted above, this investment in investigation, prosecution and adjudication capability can address the concerns expressed in the Pacific about better responding to cyber-bullying, child pornography, and the need for greater child protection online.

Capacity building in this context could also include developing a specific process for law enforcement to work with social media platforms, particularly Facebook.

In some of the smaller Pacific countries – particularly those where incidents of cybercrime are rare – it may not be practicable to train and recruit dedicated cybercrime specialists in law enforcement and prosecution services. For this reason, international cooperation links across the Pacific should be strengthened, so that this type of resource is available to low-capacity countries when required.

5 Capacity-building: regional hub

Considering the four priorities identified above, we suggest that a regional hub for cybersecurity would be valuable. This does not need to be grandiose, and it can be focussed on providing practical assistance to Pacific countries looking to put in place these fundamental cyber-security building blocks. A regional hub can be implemented in phases.

The regional hub could consolidate information, training, projects and services, and contacts, into one place. It could cover the following ground.

Collecting and sharing information:

- provide regional templates for cybersecurity strategies;
- provide regional templates for model legislation;
- provide regional templates for MOUs between enforcement agencies and stakeholders;
- share practical approaches to improving the security of essential infrastructure;
- share information on cybersecurity workshops, meetings, training course, scholarships, secondment opportunities;
- share information on risks that are being identified.

Some very early gains could be made with a simple website that collected and shared information on these key areas.

Centralising incident reporting, and Pacific-wide alerts and warnings.

Provision of services and capability to Pacific countries:

- advanced cyber incident response support for in-country teams;
- technical templates for building secure services (e.g. a template for a secure payments website);
- security and vulnerability testing services;
- centralised procurement for security and IT services;

Capacity building across the Pacific:

- The hub could be the focal point for the provision of targeted capacity building and training in cybersecurity;
- For example, it could arrange for short-term workshops on cybersecurity;
- Secondments could be offered to help local experts upskill.

We are aware that the idea for a cybersecurity centre or facility has been suggested by USP. The suggestion was that USP had already started offering cybersecurity courses and was therefore well placed to continue to provide this in the region. However, in our discussions with some Pacific stakeholders, there were strong views that the hub should not be placed at USP. Current cybersecurity courses being offered at USP were seen to be too academic (with the preference being for shorter training modules with a more practical approach), eligibility requirements too high, courses too expensive, and therefore cost prohibitive. PacCERT was based at USP and it failed to generate sustainable support. As another example, the Council of Regional Organisations of the Pacific (CROP) working group on ICT, a USP initiative, included PRIF agencies as members but this initiative and its forums were not perceived to be effective. We consider that a regional hub, sitting outside of an academic institution and with an operational focus, will better serve Pacific countries.

In our view, Vanuatu would be a good candidate to establish and build support for a hub. There are good facilities, capable people, and an existing focus on activities and services that are seen to deliver tangible value.

Priority II recommendations

6 Safeguard critical infrastructure and services

Some material gains can be made in the larger Pacific countries in managing cybersecurity risk for critical infrastructure, where digital management systems are in place. Pacific countries should be encouraged to identify operators of essential services dependent on network and/or information systems, and require these operators to take appropriate technical and organisational measures to address security issues. These security measures could be formalised either as recommended guidelines or as legislative requirements, depending on how the relevant piece of infrastructure is owned, and regulated, in the relevant country.

We would expect these measures to consider Prevention (software patching, system-level risk assessment, basic security technology like firewalls and anti-virus software), Vigilance (vulnerability scanning, security monitoring), and Resilience (off-island back-ups, CERT and incident response capability).

We expect similar infrastructure and services will be categorised as essential across the Pacific: energy, water, telecommunications, and internet providers. Some regional coordination of efforts to safeguard this infrastructure, therefore, may well be useful. This coordination could take the form of a standardised checklist for countries to follow when identifying critical infrastructure and standardised security requirements for different industries to meet. Cybersecurity should be one of the agenda items at any regional meeting of critical infrastructure providers and funders.

To the extent that regional funding is made available for security initiatives (whether or not as a consequence of the BOE Declaration), that funding could be prioritised to bring countries up to a basic standard of critical infrastructure cybersecurity.

Where foreign aid or donor funding is used to fund critical infrastructure, we recommend that funding cybersecurity steps be a required component of those projects.

7 ICT capacity-building generally across the region

The desire and need for capacity building in the Pacific is not limited to officials. Beyond law enforcement, prosecution and the judiciary, stakeholders in every country we visited identified a lack of capacity in the ICT area generally as the primary limiting factor in developing better (or any) legislative and regulatory frameworks for cybersecurity and electronic transactions.

These countries are small, often isolated, and are unable to provide remuneration packages and associated benefits that often attract talented people with an interest in cybersecurity and electronic transactions.

We recommend that the donor agencies consider how it might best incentivise and foster talent in cybersecurity and electronic transactions in the Pacific region, and more importantly to ensure that once people are trained, they remain available to assist their respective Pacific Island countries. There is a real desire for a long-term strategy on ICT capacity in the Pacific.

Some ideas for building local capacity include funding scholarships at secondary school or tertiary level, as well as scholarships for short term or extended training. In many of the Pacific Island countries that we visited, there were one or two well trained and experienced individuals, often employed in the private sector. These individuals would benefit from short term cybersecurity training, at a more advanced level. However, the majority of IT personnel placed within Ministries and organisations required, and often requested, basic cybersecurity training.

Another option would be to fund secondments to organisations in Australia, New Zealand or abroad, which would allow IT personnel to be trained in organisations operating in more established legal and

regulatory frameworks. Individuals on secondment would benefit from hands on training provided by experts within these organisations and be exposed to actual cybersecurity incidents and responses. Secondments could be made available across the region, or to a grouping of countries with similar strategies and capabilities.

We note that Digicel (operating in Samoa, Tonga, Vanuatu, Fiji, PNG and Nauru) and other ISPs in other countries are investing significantly in personnel and their cybersecurity and digital economy skills. Together with building local and/or regional CERT capability, public/private partnerships may be another way to build capacity effectively in the region.

USP and Christ's University in the Pacific both offer post-graduate cybersecurity courses. While we cannot comment on the quality of the courses, we encourage the development of "home grown" qualifications.

There may be smart ways to take advantage of the networks of talented Pacific islanders working abroad. Networks could facilitate the exchange of information, help with tailoring response to the Pacific, and with identifying and supporting new talent.

We agree with the many stakeholders who emphasised that building local capacity is essential for implementing and developing the recommendations in this report, now and into the future. As cyber threats will continue to become more sophisticated, local capacity building will need to be maintained and keep apace to deal with new threats. There will be no single answer. A Pacific strategy on ICT capacity will need to pull on as many levers as it can.

8 Privacy and data protection

Compared to more developed jurisdictions, Pacific countries tend to have fewer legislative frameworks directed at privacy and data protection regulation. Most countries have constitutional (or similar) recognition of privacy rights, but have yet to enact concrete legislative protections for the collection, use and disclosure of personal information.

However the comparison with developed jurisdictions does not in itself make this a priority. Local businesses do not appear to be collecting large amounts of personal information for marketing purposes, as is the case in other, more developed countries. Popular demand for enhanced privacy legislation is accordingly currently quite limited. That said, the public's expectations in relation to privacy may increase relatively quickly, given the increasing popularity of social media platforms and associated global publicity of privacy issues.

Before prioritising enactment of privacy legislation, it may be worthwhile investing in policy development. Two key areas were highlighted to us. First, supporting awareness-raising campaigns, so that populations in Pacific Island countries become more cognisant of the risk presented to individual privacy by mass data collection. Countries would benefit from a discussion at the local level about what they want and expect from privacy in the digital age, in the context of small Pacific state. Improved awareness should provide a platform for eventual legislative development.

Second, the size of most Pacific countries means that a standalone privacy agency is unrealistic and unnecessary. For that reason we caution against simply replicating the Australian or New Zealand privacy model for the Pacific (as has already been suggested). There is the opportunity to explore a more tailored response. An effective privacy regime requires a body capable of receiving and investigating individual complaints and which otherwise has an educative role. That body doesn't necessarily need to be a standalone body, or require extensive enabling legislation. An effective privacy and data protection function could be built into the remit of any government body which focusses on individuals, such as a department or ministry dealing with consumer issues, or a body which already has an ombudsman-type function.

The design of a privacy body, and set of privacy laws, that is appropriate for the conditions of a Pacific state, is a good design challenge. It could be grappled with at the regional level. A bespoke Pacific privacy framework, including a code and institutional framework, could be developed. As such, while individual countries focus for the next couple of years on the Priority I Building blocks for cybersecurity, perhaps this can be a focus for regional development.

9 Electronic transactions

A few Pacific Island countries have enacted direct enabling legislation for electronic transactions, drawing on the UNCITRAL Model Law on Electronic Commerce 1996 and Model Law on Electronic Signatures 2001.

Electronic transactions legislation serves primarily to confirm the legal validity of electronic communications and electronic authentication methods when parties are trading. Where there is currently no problem with the use of electronic transactions when trading, there may be less need for electronic transactions legislation.

This study has not identified any countries where electronic transactions are currently impeded due to issues of validity under domestic law. We recommend countries focus their efforts on the Priority I initiatives discussed above, for the time being.

It is possible that as electronic transactions become more widespread across the Pacific, more countries will proceed to enact this type of legislation. It is also possible that as these technologies and ways of trading become the global norm, the practical need for confirming legislation lessens. We recommend countries keep in mind the possibility of electronics transactions legislation, recognising also that the UNCITRAL model laws provide an accessible template for this type of legislation if and when required.

Detailed Policy and Legal Gap Analysis

Structure of Gap Analysis

This section reviews the policy and legal frameworks in place in each of the participating countries. It highlights the challenges and opportunities in existing legal and regulatory frameworks and offers recommendations on a way forward (at both a domestic and regional level).

In this section, we discuss cyber regulation in four key topics, drawn from the Deloitte Global Cyber Strategy Framework described in Part A.

- *strategy and governance*: the overarching policy framework for cyber-related issues;
- *cybersecurity*: the institutions, reporting systems and related processes that support cybersecurity, including the management of critical infrastructure and assets;
- *vigilance*: required reporting of cyber incidents to national competent authorities and cooperation frameworks (both domestic and international, formal and informal); and
- *resilience*: cybercrime legal frameworks (both substantive and procedural) and capacity within the criminal justice system to prosecute cybercrime.

Alongside cybersecurity, trust and confidence in a digital economy depends on an enabling legal and regulatory framework for electronic interactions. In this area, we discuss the following related topics:

- *e-transactions*: laws that enable electronic communications and transactions through ensuring non-discrimination, technological neutrality and functional equivalence;
- *privacy, freedom of speech and other human rights online*: the extent to which human rights protections apply online;
- *data protection*: laws regulating the collection, use, disclosure and storage of personal information;
- *digital authentication*: laws governing systems that enable the creation and assertion of digital identities;
- *ccTLD administration*: administration and regulation of top level domains to encourage growth in a digital economy;
- *consumer protection*: laws prohibiting unfair or deceptive business practices, including online;
- *intellectual property legislation*: laws necessary to adequately protect content creators; and
- *access to information*: laws, guidelines and principles designed to facilitate the free-flow of information, including from government.

Summary of Country-level Findings

Stage of development	None	Initial	Established	Sophisticated

Country	CI	FJ	FSM	KI	RMI	NR	NU	PW	PNG	WS	SB	TO	TV	VU
Strategy and governance														
National cybersecurity strategy	I	E	I	I	N	I	N	N	E	E	N	I	I	E
Governance	I	E	I	E	I	E	I	N	E	E	N	E	E	E
Security														
Institutions	I	I	I	I	I	I	I	N	E	E	N	E	I	E
Critical infrastructure	I	N	N	N	N	N	N	N	N	I	N	E	N	I
Vigilance														
Incident reporting	I	I	I	N	N	I	I	I	I	N	I	I	I	I
Domestic cooperation	I	E	N	I	N	E	N	N	I	E	N	I	N	I
International cooperation	E	I	I	I	I	E	I	I	I	I	I	E	I	E
Resilience														
Cybercrime (substantive)	I	E	N	E	I	S	N	I	S	E	I	E	I	I
Cybercrime (child protection)	I	N	N	E	I	S	I	E	E	E	N	E	N	E
Cybercrime (procedural)	I	I	I	E	I	S	I	I	S	I	I	E	I	I
Law enforcement	I	I	I	I	I	I	I	I	I	I	I	I	I	I
Prosecution	I	I	I	I	I	I	I	I	I	I	I	I	I	I
Courts	I	I	I	I	I	I	I	I	I	I	I	I	I	I
Legal and regulatory frameworks														
Electronic transactions	I	E	N	N	N	N	N	N	N	E	N	N	N	E
Privacy, freedom of speech and other human rights online	I	I	I	I	E	I	N	I	I	I	I	N	I	I
Data protection	N	I	N	N	I	N	N	I	I	I	N	I	N	I
Digital authentication	I	N	N	N	I	N	N	N	I	I	N	I	N	N
ccTLD administration	E	E	E	E	I	E	E	E	I	E	I	I	E	I
Consumer protection	S	E	N	E	E	I	I	E	E	E	I	E	N	I
Intellectual property legislation	E	E	E	I	I	I	E	E	E	E	N	E	I	E
Access to information	E	E	N	I	I	I	N	E	N	I	N	I	I	E

Note: "Initial" means that the country is in the process of developing or implementing the concept measured and "Established" refers to a state where the relevant framework or concept is implemented and operates. Each of these ratings refers to the particular concept measured, and not the country's overall capacity to respond to cyber-risk.

Cook Islands

Summary

The Cook Islands Government has set a strategic direction to centralise and improve ICT infrastructure as a part of the National Sustainable Development Plan (2016-2020) and the e-Government Strategy (2013-2018). The Cook Islands also has a National Information and Communication Technology Policy, developed in July 2015, which acknowledges the threat presented by cybercrime and sets out an intention to strengthen the Cook Islands' cybercrime regulatory framework accordingly. No specific cybersecurity policy or strategy is in place.

The Telecommunications Act 1989 includes some cybercrime provisions relating to interference with telecommunications. A draft Crimes Bill, prepared in 2017, contains a well-developed set of cybercrime provisions, drawing on the Budapest Convention.

The Cook Islands also has well-developed consumer protection and intellectual property legislation, contributing to a regulatory framework for safeguarding electronic transactions.

To give a sense of scale, an estimate of the size of the population in the Cook Islands is 17,400 people.

Cybersecurity

Strategy and governance		
National cybersecurity strategy	*Initial*	A National Information and Communication Technology Policy was developed in 2015. This policy acknowledges the threat presented by cybercrime and cyber-bullying. It focusses on improving government cybersecurity awareness, strengthening the cybercrime regulatory framework and working with partners of the Cook Islands to manage cybersecurity risk. The National Sustainable Development Plan (2016-2020) and the e-Government Strategy (2013-2018) also support improvements to ICT infrastructure. The National ICT Office within the Office of the Prime Minister has been tasked with developing a specific cybersecurity strategy, although work on this document has not yet begun. There is no formal stakeholder arrangement for this process, but the Ministry of Finance, the Office of the Prime Minister, Crown Law, the Cook Islands Police and Bluesky (a local telecommunications company) are all likely to be involved.
Governance	*Initial*	The National ICT Office has responsibility for ICT issues generally, including cybersecurity. Crown Law and the Cook Islands Police also have significant involvement in cybersecurity matters.
Security		
Institutions	*Initial*	As above, the National ICT Office, Crown Law and the Cook Islands Police work jointly on cybersecurity issues. The Cook Islands has not established a CERT, due to lack of resources. The Cook Islands was a participant in PacCERT, while it was operational, and considered that project to be of significant value to smaller Pacific countries, which lack the size and resources to run their own CERTs.

Critical infrastructure	*Initial*	No cybersecurity arrangements for critical infrastructure identified. The primary operators of critical infrastructure in the Cook Islands (Bluesky, Cook Islands Investment Cooperation and TeApongaUira) manage their own cybersecurity, but expressed an interest in developing standardised cybersecurity guidelines and recommendations for this purpose.
Vigilance		
Incident reporting	*Initial*	No cybersecurity incident reporting requirements identified.
Domestic cooperation	*Initial*	An informal ICT working group is composed of representatives from the Office of the Prime Minister, Crown Law and the Police. The Ministry of Finance and Bluesky are also involved as stakeholders. The Cook Islands is a participant in the Cyber Safety Pasifika programme, and has arranged cyber safety presentations in most of the country's schools, targeted at students, teachers and parents.
International cooperation	*Established*	The Cook Islands is a member of PaCSON, PICISOC, PICP and PTCN. The Cook Islands is also an associate member of the APT, a non-participating country of the PIRRC (receiving indirect benefits) and is among the beneficiaries of the ICB4PAC project. Links to New Zealand and Australia are strong, including to AFP (with the Pacific Police Development Program) and New Zealand Police (with the Pacific Island Prevention Programme). The Cook Islands would likely call on New Zealand's CERT for any necessary assistance following a cyber incident. The Extradition Act 2003 and the Fugitive Offenders Act 1969 provide for extensive extradition powers, for offences with a maximum penalty of at least one year's imprisonment. The Mutual Assistance in Criminal Matters Act 2003 provides for mutual legal assistance, for offences with a maximum penalty of at least one year's imprisonment.
Resilience		
Cybercrime (substantive)	*Initial*	The Telecommunications Act 1989 creates offences for forging a telecommunications message, intercepting telecommunications messages and interference with telecommunications. The Spam Act 2008 prohibits the sending of unsolicited commercial electronic messages and prescribes certain requirements for commercial electronic messages. A new Crimes Bill was prepared in 2017, drawing heavily on the Australian Model Criminal Code. This Bill includes a comprehensive set of cybercrime offences and cybercrime procedural powers, modelled on the Budapest Convention. A Parliamentary select committee is currently considering the Bill, and it is then expected to proceed for enactment.
Cybercrime (child protection)	*Initial*	The Crimes Act 1969 creates an offence for creation, exhibition or delivery of indecent documents, which presumably can apply to child abuse material. The new Crimes Bill 2017 includes a comprehensive set of offences relating to child abuse and other indecent material. The Cook Islands has acceded to the Convention on the Rights of the Child.

Cybercrime (procedural)	*Initial*	The Criminal Procedure Act 1980-81 contains general search and seizure powers. The new Crimes Bill 2017 includes a comprehensive set of cybercrime procedural powers, including powers relating to production orders, preservation of data, collection and disclosure of traffic data and interception. There are some concerns among telecommunications providers that it will not be technically possible to collect the information required under these provisions.
Law enforcement	*Initial*	The Cook Islands Police do not have sufficient personnel and funding resources to investigate and prosecute cybercrime offences. The Cook Islands can utilise the PTCCC, based in Samoa. The Cook Islands can also draw on law enforcement resources from the AFP, New Zealand Police and SFO when required.
Prosecution	*Initial*	Prosecution for cybercrime matters will be the responsibility of either Crown Law or the Police (determined on a case by case basis). The ability to effectively prosecute these offences will depend on appropriate investigation and collection of evidence.
Courts	*Initial*	No issues with judicial capacity to accept and understand electronic evidence have been identified.

Safeguarding electronic transactions

Legal and regulatory frameworks		
Electronic transactions	*Initial*	The Digital Registers Act 2011 regulates the use of digital registers, where the register is established under an enactment. This Act makes provision for digital copies of registers to prevail over hard copies, with certain exceptions, and allows digital copies of registers to be admitted as evidence. No general enabling legislation for electronic transactions identified.
Privacy, freedom of speech and other human rights online	*Initial*	The Cook Islands Constitution, via the Constitution Amendment (No 9) Act 1980-81, recognises certain fundamental human rights, including freedom of thought and conscience, and freedom of speech and expressions. There is no constitutional right to privacy.
Data protection	*None*	No general privacy or data protection regulation identified.
Digital authentication	*Initial*	No current digital authentication system, although an e-government project is underway and digital authentication will likely be a part of this work. The Digital Registers Act 2011 sets out a number of requirements for creating and maintaining a digital register (where that register is established under an enactment).
ccTLD administration	*Established*	The Cooks Islands ccTLD is .ck and is managed by Telecom Cook Islands Ltd (Bluesky).

Legal and regulatory frameworks		
		Bluesky has prepared a dispute resolution procedure, modelled on a policy used for New Zealand's ccTLD (.nz), but this procedure has not yet needed to be used.
Consumer protection	*Established*	The Ministry of Internal Affairs has responsibility for consumer protection in the Cook Islands. Relevant legislation includes the Consumer Guarantees Act 2008, Fair Trading Act 2008, Control of Prices Act 1966 and Small Claims Tribunal Act 2008.
Intellectual property legislation	*Established*	The Cook Islands has a Copyright Act 2013, which includes offences for intentional copyright infringement. The Traditional Knowledge Act 2013 provides for legal recognition of traditional knowledge and a registration process to establish rights to traditional knowledge. Under the Cook Islands Act 1915, the New Zealand Patents Act 1953, Designs Act 1953 and Trade Marks Act 1953 are also in force in the Cook Islands.
Access to information	*Established*	The Official Information Act 2008 provides for public access to official information. The Ombudsman of the Cook Islands has powers to investigate and review decisions to refuse an access request for official information. Crown Law will provide advice on requests for official information, as requested.

Recommendations

The latest official published population statistics for the Cook Islands (in 2016) estimated less than 12,000 people lived in the islands. For that reason, the extent to which the Cook Islands can, or needs, to effectively enforce its comprehensive framework of laws and regulations is an open question. In our view, continuing close cooperation and assistance from New Zealand and Australia on cyber issues is the most effective and efficient path for the Cook Islands. In particular, ensuring that the Cook Islands continues to have access to cyber risk identification, mitigation and education resources from New Zealand and Australia.

On the basis of our desktop review and consultation mission to the Cook Islands, our recommendations are as follows:

- *Develop a cybersecurity strategy*: The National ICT Office and Crown Law office should develop a national cybersecurity strategy, identifying relevant risks, and a plan to strengthen the Cook Islands' cyber framework. The strategy could also identify critical infrastructure, and a system for monitoring and reporting on threats and vulnerabilities. One option may be to develop this strategy as part of a revised National ICT Policy.
- *Continue legislative enactment process*: The Cook Islands should continue the enactment process for the new Crimes Bill 2017, bringing its cybercrime legislation into line with the Budapest Convention.
- *Improve capacity levels and international cooperation*: Once the new legislation is enacted, the Cook Islands' major challenge will be to ensure law enforcement and prosecutorial capacity is sufficient to implement the legislation and prosecute cybercrime as it occurs. Improving this capacity is likely to involve a combination of training and allocation of resources, together with continuing to develop links with law

enforcement counterparts in Australia and New Zealand, so that specialised assistance is accessible when needed.

- *Develop a legislative framework for a digital economy*: The Cook Islands has an established consumer protection, intellectual property and access to information legislative framework, but has not yet developed direct electronic transactions, privacy or data protection legislation. While this is a lower priority and the focus should remain on cybersecurity, development of this framework can remain on the agenda for when the capacity for reform is available and the need is established.

Federated States of Micronesia

Summary

The Federated States of Micronesia (*FSM*) does not have a published cybersecurity strategy, although the National ICT and Telecommunications Policy 2012 sets out some objectives relating to cybersecurity. FSM does not currently have specific cybercrime or electronic transactions laws. FSM is involved in the Cyber Safety Pasifika programme and, in association with this programme, has conducted some cybersecurity awareness-raising activities.

To give a sense of scale, an estimate of the size of the population in the FSM is 106,200 people.

Cybersecurity

Strategy and governance		
National cybersecurity strategy	*Initial*	FSM has no published cybersecurity strategy. FSM does have a National ICT and Telecommunications Policy, created in 2012, which contains some cyber-related strategy. In particular, the strategy includes an objective of protecting "citizens' rights relating to cybercrime, child protection and the right to information", under "Goal 4: Utilize ICT for Good Governance".
Governance	*Initial*	The Department of Transportation, Communication and Infrastructure (*TC&I*) is in charge of telecommunications and the FSM government IT network. TC&I will accordingly be an important stakeholder in FSM's cybersecurity policy, although cybersecurity does not appear to be a specific item on its mandate.
Security		
Institutions	*Initial*	As above, TC&I has some responsibility for cybersecurity in FSM, flowing from its role as the government agency in charge of telecommunications and the government IT network. Other government agencies with an interest in cybersecurity matters include the Public Auditor, the Attorney-General / Department of Justice, the Department of Finance and the National Police.
Critical infrastructure	*None*	No cybersecurity arrangements for critical infrastructure identified.
Vigilance		
Incident reporting	*None*	No cybersecurity incident reporting requirements identified.
Domestic cooperation	*None*	No formal cybersecurity cooperation procedures are in place. FSM has conducted some awareness raising campaigns, including participating in the Cyber Safety Pasifika programme.
International cooperation	*Initial*	FSM is a member of APT, PICISOC, PICP, PITA and PTCN. FSM is not a member of PaCSON. FSM is a member of the Cyber Safety Pasifika programme. FSM is a participating country for PIRRC and is among the beneficiary countries of the ICB4PAC project, receiving support in relation to the development of FSM's National ICT and Telecommunications Policy.

		The FSM National Police regularly cooperate with the FBI in Guam and/or Hawaii, especially for criminal cases involving the United States. There are also some links between the FSM National Police and the AFP (under the Pacific Police Development Program) and the New Zealand Police. Title 12 contains provisions for extradition and mutual legal assistance. There is no offence threshold for extradition. For mutual legal assistance, the offence must have a maximum penalty of at least one year's imprisonment.
Resilience		
Cybercrime (substantive)	*None*	A Cybercrime Bill was submitted to the FSM Congress in 2016, but has not been enacted into law. We understand this Cybercrime Bill is in a process of revision, to reflect recent developments in cybercrime legislation.
Cybercrime (child protection)	*None*	FSM does not appear to have legislation for online child protection, although some child protection provisions may be included in the draft Cybercrime Bill (we have not been able to confirm this). FSM has acceded to the Convention on the Rights of the Child and has signed and ratified the Optional Protocol on the Sale of Children, Child Prostitution and Child Pornography.
Cybercrime (procedural)	*Initial*	Criminal Procedure [Title 12] provides for general search and seizure. Further procedural powers may be included in the draft Cybercrime Bill, although we have not been able to confirm this.
Law enforcement	*Initial*	The FSM National Police does not have a dedicated cybercrime unit, although there has been some discussion about establishing one. FSM has experienced a few cases of hacking and computer-facilitated fraud. Some cybercrime training has been provided to members of the FSM National Police, including through annual PILON workshops. We understand the National Police would like further assistance and training in this area.
Prosecution	*Initial*	We expect prosecution capacity to be low, given the limited cybercrime training for the police and the lack of cybercrime prosecutions.
Courts	*Initial*	We expect judicial capacity to be low, given the limited cybercrime training for the police and the lack of cybercrime prosecutions.

Safeguarding electronic transactions

Legal and regulatory frameworks		
Electronic transactions	*None*	No general enabling legislation for electronic transactions identified.
Privacy, freedom of speech and other human rights online	*Initial*	The Constitution of FSM includes a declaration of rights. In particular, section 5 sets out a right of the people to be secure against unreasonable search, seizure and invasion of privacy. Some complaints made to the National Police or legal services about privacy issues.

Legal and regulatory frameworks		
Data protection	*None*	No general privacy or data protection legislation identified.
Digital authentication	*None*	No digital authentication system identified.
ccTLD administration	*Established*	The .fm domain name is managed by FSM Telecommunications Corporation. This domain appears to be used by a number of FM radio services located outside FSM. BRS Media, Inc. manages registration of second-level domains under the .fm domain, and has adopted ICANN's Uniform Domain Name Dispute Resolution Policy.
Consumer protection	*None*	No consumer protection legislation identified.
Intellectual property legislation	*Established*	Title 35 (Copyright, Patents and Trademarks) provides for intellectual property rights, including offences for copyright infringement that may extend to electronic material.
Access to information	*None*	No access to information legislation identified.

Recommendations

On the basis of our desktop review and discussions with FSM representatives, our recommendations are as follows:

- *Develop cybersecurity strategy*: FSM could consider developing a cybersecurity strategy, sitting alongside its ICT policy, to specifically identify key risks and priority actions to strengthen FSM's ability to detect and respond to cyber incidents. The strategy should identify an agency responsible for cybersecurity (presumably TC&I), and outline the functions and responsibilities of related agencies.
- *Progress the draft Cybercrime Bill*: FSM should continue development of the draft Cybercrime Bill, drawing on the Budapest Convention as a precedent. Alongside new legislation, it will be important to ensure that the police, prosecutors and the judiciary are adequately resourced and trained to deal with cyber cases.
- *Legislative support for a digital economy*: FSM lacks the traditional legislative and regulatory support for a digital economy, including, in particular, laws providing for the equivalency and legal validity of electronic transactions and for the regulation of collection, use and disclosure of personal information. In our view the priority area of reform is cybersecurity. However the development of these laws should remain on the agenda for the time when capacity for reform is available, and these laws are needed to support the increasing use of technology and electronic transactions by its citizens.

FSM has a continuing close association to the United States. Our recommendations anticipate that with respect to cybercrime, FSM would continue to receive the benefit of assistance and advice from the United States (and, in particular, the FBI). However, we do recommend that with respect to strategy and enforcement of legislative frameworks, FSM continues to benefit from regional associations and assistance.

Fiji

Summary

Fiji has taken steps to establish a governance framework for cybersecurity, and to develop a national cybersecurity strategy and cybercrime legislation. Further reform of cybercrime legislation is also underway, although we have not been able to confirm the current status of this project.

The Fiji Police Force has a dedicated Cybercrime Investigations Unit, equipped to investigate and respond to cybercrime incidents.

Fiji also has a relatively comprehensive legislative framework for safeguarding electronic transactions, although further consideration should be given to privacy and data protection regulation, as collection of personal information increases.

To give a sense of scale, an estimate of the size of the population in Fiji is 912,200 people.

Cybersecurity

Strategy and governance		
National cybersecurity strategy	*Established*	Fiji appears to have developed a draft National Cybersecurity Strategy, in collaboration with the CTO. We have not been able to confirm the current status of this document. Fiji also has a National Broadband Policy 2011, although this document does not make any express reference to cybersecurity matters.
Governance	*Established*	The Ministry of Defence and National Security appears to have general responsibility for cybersecurity matters. Other relevant stakeholders include the Department of Communications (which is responsible for ICT in Fiji), the Office of the Attorney-General, the Office of the Director of Public Prosecutions and the Police Force.
Security		
Institutions	*Established*	As above, the Ministry of Defence and National Security appears to have general responsibility for cybersecurity matters. Fiji does not have a CERT.
Critical infrastructure	*None*	No cybersecurity arrangements for critical infrastructure identified.
Vigilance		
Incident reporting	*Initial*	Cybercrime incidents can be reported to the Police Force and are registered by the Cybercrime Investigation Unit. No cybersecurity incident reporting requirements identified.
Domestic cooperation	*Established*	In 2010, Fiji formed a Cybersecurity Working Group, led by representatives from the Police Force and the Ministry of Defence. It also included government IT departments, network service providers

		and banks. We have not been able to confirm the current status of this group.
International cooperation	*Initial*	Fiji is a member of APT, CTO, Interpol, PaCSON, PICISOC, PICP, PITA and PTCN. Fiji is a participating country for the PIRRC and is among the beneficiaries of the ICB4PAC project. The Extradition Act 2003 provides for extradition processes, for offences with a maximum penalty of at least one year's imprisonment. The Mutual Assistance in Criminal Matters Act 1997 provides for mutual legal assistance, for offences with a maximum penalty of at least one year's imprisonment.
Resilience		
Cybercrime (substantive)	*Established*	The Crimes Decree 2009: Part 17, Division 6 - Computer Offences includes a number of cybercrime-related offences, including unauthorised modification of data, unauthorised access to restricted data and unauthorised impairment of electronic communication or data. Part 11 of the Crimes Decree 2009 also sets out a number of general forgery offences, without specific application to cybercrime. The Posts and Telecommunications Decree 1989 includes offences relating to telecommunications systems, including interception and disclosure of messages, altering messages, and fraudulent and improper use of a telecommunications system. The Ministry of Defence and National Security began drafting a Cyber Crime Decree in 2016. We have not been able to confirm the current status of this legislation.
Cybercrime (child protection)	*None*	Other than general sexual abuse offences, Fiji does not have child protection legislation. Fiji has signed and ratified the Convention on the Rights of the Child. Fiji has also signed the Optional Protocol on the Sale of Children, Child Prostitution and Child Pornography.
Cybercrime (procedural)	*Initial*	There is no specific procedural cybercrime legislation. The Posts and Telecommunications Decree 1989 provides for regulations to be made for the preservation of electronic messages, although we are not aware of any such regulations in existence. This Decree also provides for the production of electronic messages by warrant. Part IX of the Criminal Procedure Decree 2009 provides for general search and seizure powers. The Telecommunications Promulgation 2008 requires service providers supplying telecommunications to disclose information to government authorities for enforcing criminal laws and protecting the public interest, and gives the Telecommunications Authority of Fiji the power to require disclosure of information and documents reasonably required by it.

Law enforcement	*Established*	The Fiji Police Force has established a dedicated Cyber Crime Investigations Unit, with including trained investigators and technical officers, and the capacity to conduct computer and mobile forensics investigations. We have not been able to confirm the current status of this unit.
Prosecution	*Initial*	We expect prosecution capacity to be low, given the absence of a full cybercrime framework and limited enforcement activity.
Courts	*Initial*	We expect judicial capacity to be low, given the absence of a full cybercrime framework and limited enforcement activity.

Safeguarding electronic transactions

Legal and regulatory frameworks		
Electronic transactions	*Established*	The Electronic Transactions Act 2008 and the Electronic Transactions (Amendment) Act 2017 contain general enabling provisions for electronic transactions and electronic signatures.
Privacy, freedom of speech and other human rights online	*Initial*	The Fiji Constitution recognises fundamental rights to freedom from unreasonable search and seizure, freedom of speech, expression and publication, freedom of association and the right to privacy.
Data protection	*Initial*	The Telecommunications Promulgation 2008 provides that any telecommunications service provider supplying telecommunications to consumers must keep information about consumers confidential, including billing information and call information, except to the extent necessary to publish any public telecommunications directory, enable billing or to address fraud or bad debt. No general privacy or data protection legislation identified.
Digital authentication	*None*	There is no national identification or digital authentication system in Fiji. Proposals to introduce a compulsory identity card were made in 2010, but do not appear to have progressed.
ccTLD administration	*Established*	The .fj domain name is administered by the University of the South Pacific. The Uniform Domain Name Dispute Resolution Policy applies.
Consumer protection	*Established*	The Fair Trading Decree 1992 and the Consumer Credit Act 1999 provide for consumer protection in Fiji. The Commerce Act 1998 provides for certain market regulation, including price control. The Telecommunications Promulgation 2008 requires service providers to comply with certain consumer protection rules, including not making any false or misleading statements or representations.
Intellectual property legislation	*Established*	Intellectual property rights are protected via a range of legislation: the Copyright Act 1999 (which includes offences for dealing with infringing objects), the Patents Act and Patents (Amendment) Act 2002 and the Trade Marks Act 1978.

Legal and regulatory frameworks		
Access to information	*Established*	The Information Act 2018 provides for public access to official information, with the Accountability and Transparency Commission to determine whether to accept any information request. The Public Service Act 1999 also mandates that an employee must not make improper use of official information or any information about public business.

Recommendations

On the basis of our desktop review and a consultation visit to Fiji, our preliminary recommendations are as follows:

- *Strengthen cybercrime legal framework:* Fiji's current cybercrime legislation has significant gaps, particularly in relation to child protection and procedural powers. We recommend continuing with the process to enact a new Cybercrime Act, using the provisions of the Budapest Convention as a guide. At the same time, it is also important to ensure the police have adequate resourcing to investigate cybercrimes, and that resourcing and training is also available to prosecutors and the judiciary in relation to cybercrime cases.
- *Develop an incident response capability*: With governance and cooperation frameworks reasonably well-established, Fiji should focus on using these frameworks to enable an effective response to cybersecurity incidents as and when these occur. This may involve developing rules and procedures for incident reporting, particularly for any incidents affecting critical infrastructure, and establishing a national CERT or similar capability.
- *Consider developing a privacy and data protection framework*: Fiji already has a robust framework for e-transactions and consumer protection. To complement this framework, Fiji should start to raise awareness of privacy issues associated with new technology and, eventually, should consider developing privacy and data protection legislation, to regulate the collection, use and disclosure of personal information.

Kiribati

Summary

Kiribati has a National ICT Policy but no specific cybersecurity policy or strategy. Some cyber-related offences are set out in the Communication (Amendment) Act 2016, although these are not comprehensive.

Kiribati also has some consumer protection and intellectual property legislation in place, with plans to further develop its legislative framework for electronic transactions.

To give a sense of scale, an estimate of the size of the population in Kiribati is 118,400 people.

Cybersecurity

Strategy and governance		
National cybersecurity strategy	*Initial*	The Kiribati National ICT Policy, developed in 2011, notes an intention to expand the policy to cover cybersecurity, together with e-commerce, e-government and privacy. Kiribati intends to update the current National ICT Policy, as part of a broader project to develop the Kiribati telecommunications and ICT sector. This project is supported by the World Bank.
Governance	*Established*	The Ministry of Information, Communication, Transport and Tourism Development (*MICTTD*) has an ICT policy and development division. This division is responsible for ICT and related matters, including cybersecurity and awareness-raising programmes. Other stakeholders on cybersecurity matters include the Office of the Attorney-General and the Kiribati Police Force.
Security		
Institutions	*Initial*	As above, MICTTD is responsible for cybersecurity policy. Kiribati does not have a CERT in operation.
Critical infrastructure	*None*	No cybersecurity arrangements for critical infrastructure identified.
Vigilance		
Incident reporting	*Initial*	No cybersecurity incident reporting requirements identified.
Domestic cooperation	*Initial*	Kiribati established a government ICT working group in 2016, which functions as a coordination mechanism for the ICT representatives from each government ministry and state-owned enterprise. No other domestic cooperation procedures identified.
International cooperation	*Initial*	Kiribati is a member of APT, PaCSON, PICISOC, PICP, PITA and PTCN. Kiribati is a participating country for the PIRRC and is among the beneficiaries of the ICB4PAC project.

		Kiribati takes part in the Cyber Safety Pasifika programme, although we understand awareness-raising programmes in Kiribati are limited. The Kiribati Police have some links to the AFP (under the Pacific Police Development Program) and New Zealand Police (under the Pacific Island Prevention Programme). The Extradition Act 2003 sets out rules and procedures for extradition, applicable to offences with a maximum penalty of at least one year's imprisonment. The Mutual Assistance in Criminal Matters Act 2003 contains reasonably extensive provisions for mutual assistance, including search and seizure powers and evidence protection. This Act applies to offences with a maximum penalty of at least one year's imprisonment.
Resilience		
Cybercrime (substantive)	*Established*	The Communications Act 2012 and the Communication (Amendment) Act 2016 contain a number of cybercrime offences, including for unauthorised access to computer material, unauthorised modification of computer material, unauthorised use of a computer service, unauthorised access to data, unauthorised interception, computer-related forgery and computer-related fraud. Prior to its repeal under the Communications Act 2012, the Telecommunications Act 2004 also contained offences relating to the interception of messages, computer misuse, offensive messages and obscene material. Part XXXVI of the Penal Code contains provisions relating to general fraud and forgery.
Cybercrime (child protection)	*Established*	The Communications Act 2012 includes offences for the distribution and exhibition of obscene matter, and the production, distribution and possession of child abuse material. Kiribati has acceded to the Convention on the Rights of the Child and to the Optional Protocol on the Sale of Children, Child Prostitution and Child Pornography.
Cybercrime (procedural)	*Established*	The Communications Act 2012 contains a number of procedural provisions relating to investigations and the collection of evidence. These provisions include powers relating to search warrants, information requests by the Communications Commission, required interception or disclosure of communications, real-time collection of data and witness examinations. There are also general search and seizure powers set out in the Criminal Procedure Code.
Law enforcement	*Initial*	No cybercrime prosecutions have yet been conducted in Kiribati, and relatively few complaints are made to the Kiribati Police over cyber-related issues. Law enforcement capacity is accordingly expected to be low.
Prosecution	*Initial*	We expect prosecution capacity to be low, given the limited cybercrime training for the police and the lack of cybercrime prosecutions.

Courts	*Initial*	We expect judicial capacity to be low, given the limited cybercrime training for the police and the lack of cybercrime prosecutions.

Safeguarding electronic transactions

Legal and regulatory frameworks		
Electronic transactions	*None*	No general electronic transactions enabling legislation identified. Kiribati has recently requested that a "Rapid e-Trade Readiness Assessment" be conducted by UNCTAD.
Privacy, freedom of speech and other human rights online	*Initial*	The Kiribati Constitution sets out various fundamental rights, including the rights to freedom of conscience, freedom of expression, freedom of assembly, freedom of association and protection for the privacy of the home and property. The National ICT Policy 2011 notes an intention to expand the policy to address privacy matters.
Data protection	*None*	No general privacy or data protection legislation identified.
Digital authentication	*None*	No current digital authentication system identified. Kiribati is investigating options for e-government (under the World Bank Telecommunications and ICT Development Project), which may involve development of a digital authentication system.
ccTLD administration	*Established*	Kiribati's ccTLD is .ki. This domain is managed by the Ministry of Communications, Transport and Tourism Development. In practice, the domain appears to be little-used. The Uniform Domain Name Dispute Resolution Policy applies.
Consumer protection	*Established*	Consumer protection is provided for in the Consumer Protection Act 2001, including the publication of product standards, prohibitions on misleading and deceptive conduct and statutory warranties.
Intellectual property legislation	*Initial*	The Copyright Ordinance provides penalties for dealing with infringing copies of works and for copies of works infringing copyright in the United Kingdom to be restricted from importation into Kiribati. The Communications Act 2012, section 112, provides that knowing breach of copyright by means of a computer is an offence. Kiribati also has a Registration of United Kingdom Trade Marks Ordinance, United Kingdom Design Protection Ordinance and Registration of UK Patents Ordinance.
Access to information	*Initial*	Kiribati has a Communications and Access to Information Strategy, but no legislation providing for access to official information.

Recommendations

On the basis of our desktop review and discussions with Kiribati representatives, our recommendations are as follows:

- *Develop a cybersecurity strategy:* Kiribati should develop a national cybersecurity strategy, identifying relevant risks, and a plan to strengthen Kiribati's cyber framework. The strategy could also identify critical infrastructure, and a system for monitoring and reporting on threats and vulnerabilities. It may be simplest to develop this strategy as part of a revised National ICT Policy.
- *Strengthen cybercrime framework*: Kiribati has an established cybercrime framework, but should explore whether more comprehensive reform might be useful or appropriate to bring the law in line with the Budapest Convention. In particular, expanded child protection offences and more developed procedural powers may be useful. In tandem, Kiribati should focus on ensuring that officials within the criminal justice system are resourced and trained to deal with cyber cases (including in law enforcement, prosecutors and the judiciary).
- *Develop a legislative framework for a digital economy*: Kiribati has an established consumer protection framework and has constitutional privacy rights, but otherwise has a relatively undeveloped legal framework to support e-commerce. Development of this framework should stay on the agenda, as a lower priority to other recommendations, for a time when reform capacity is available and there is the need for this support for the use of technology and electronic transactions by Kiribati citizens.

Nauru

Summary

Nauru has relatively sophisticated cybercrime legislation in place through the Cybercrime Act 2015, providing for a variety of computer-related offences and associated procedural powers, modelled on the Budapest Convention. Child protection legislation is also relatively comprehensive.

Nauru is developing domestic cybersecurity institutions and cooperation frameworks, including the Cybercrime Task Force and a Cybercrime Unit within the Nauru Police Force. Continued focus on increasing the capacity of these organisations will be important to ensure they are able to operate effectively.

Nauru's legislative framework for safeguarding electronic transactions appears relatively underdeveloped.

To give a sense of scale, an estimate of the size of the population in Nauru is 11,300 people.

Cybersecurity

Strategy and governance		
National cybersecurity strategy	*Initial*	Nauru's National Sustainable Development Strategy 2005-2025 includes some ICT matters, but does not specifically refer to cybersecurity. A National ICT Policy was in development in 2011. We have not been able to confirm the current status of this document. A previous study also mentions an effort to develop a National Cybersecurity Strategy, although, again, we have not been able to confirm the status of this document.
Governance	*Established*	The Government of Nauru has an Information and Communications Technology Department, located under the Ministry of Telecommunications. Cybersecurity does not appear to be a specific item on the ICT Department's mandate, but will likely fall within its sphere of responsibility. Other relevant stakeholders include the Department of Justice and Border Control, the Prosecutions Office and the Police Force. Nauru has also established a Cybercrime Task Force (comprised of representatives of the ICT Department, the Department of Justice and Border Control, and the Nauru Police Force) and a Cybercrime Unit within the Nauru Police Force.
Security		
Institutions	*Initial*	As above, the Nauru ICT Department is likely to be responsible for cybersecurity policy. Nauru does not have a CERT.
Critical infrastructure	*None*	No cybersecurity arrangements for critical infrastructure identified.
Vigilance		

Incident reporting	*Initial*	Cybercrime incidents appear to be reported to police. No cybersecurity incident reporting requirements identified.
Domestic cooperation	*Established*	The Cyber Safety Task Force, if still current, is likely to be the primary domestic co-operation forum. No other formal domestic cooperation arrangements identified.
International cooperation	*Established*	Nauru is a member of APT, Interpol, PICISOC, PICP and PITA. Nauru does not appear to be involved in PaCSON. Nauru is a participant in Cyber Safety Pasifika, conducting a community-wide awareness-raising campaign under this programme. Nauru is a non-participating country of the PIRRC (receiving indirect benefits), is part of the ITU-Impact Initiative and is among the beneficiaries of the ICB4PAC project. Nauru has some international law enforcement links, including a direct cooperation programme with the AFP. The Mutual Assistance in Criminal Matters Act 2004 contains rules and procedures for mutual legal assistance in criminal matters, for offences with a maximum penalty of at least one year's imprisonment. The Extradition of Fugitive Offenders Act 1973 provides rules and procedures for extradition, for a limited list of offences with a maximum penalty of at least one year's imprisonment. These offences do not currently include cybercrime and other cyber-enabled offences.
Resilience		
Cybercrime (substantive)	*Sophisticated*	The Cybercrime Act 2015 is modelled on the Budapest Convention and creates various computer offences including illegal access, interception, data interference, data espionage, system interference and distributing/possessing software or a device for committing a crime. The Act also contains provisions relevant to the liability of ISPs. The Telecommunications Act 2002 also prohibits intercepting, using, disclosing or interfering with communications and sending obscene, indecent or menacing communications. The Crimes Act 2016 contains various offences that can be conducted by electronic means, including pornography, taking images of private acts, fraud, forgery and identity crime. The Domestic Violence and Family Protection Act 2017 includes an offence for stalking a former domestic partner through persistently sending emails or messages using the internet.
Cybercrime (child protection)	*Sophisticated*	The Cybercrime Act 2015 includes offences for child abuse material, solicitation of children and publishing indecent or obscene information or material. The Crimes Act 2016 includes offences for taking images of private acts, child sexual abuse, and dealing with child abuse material. Nauru has acceded to the Convention on the Rights of the Child. Nauru also signed, but did not ratify, the Optional Protocol on the Sale of Children, Child Prostitution and Child Pornography.

Cybercrime (procedural)	*Sophisticated*	The Cybercrime Act 2015 contains detailed procedural powers, drawn from the Budapest Convention. These include: • provisions for production orders and expedited preservation of data; • search and seizure powers specific to electronic evidence, including collection of traffic data; and • provisions for interception of content data where reasonably required for the purposes of a criminal investigation and use of remote forensic tools.
Law enforcement	*Established*	A Cybercrime Unit has been established within the Nauru Police Force. Several prosecutions have occurred under the Cybercrime Act 2015, with at least three convictions.
Prosecution	*Initial*	Cybercrime prosecutions are handled by the Prosecutions Office (including the Director of Public Prosecutions). We expect prosecutorial capacity for cybercrime cases to be low, though probably higher than some other Pacific countries, given the cybercrime prosecutions that have occurred.
Courts	*Initial*	We expect judicial capacity to be low, though probably higher than some other Pacific countries, given the cybercrime prosecutions that have occurred.

Safeguarding electronic transactions

Legal and regulatory frameworks		
Electronic transactions	*None*	No general enabling legislation for electronic transactions identified.
Privacy, freedom of speech and other human rights online	*Initial*	The Nauru Constitution recognises as fundamental rights, freedom of conscience, freedom of expression, freedom of peaceful assembly and association, and respect for private and family life.
Data protection	*None*	No general privacy or data protection legislation identified.
Digital authentication	*None*	No digital authentication system identified.
ccTLD administration	*Established*	Nauru's ccTLD is .nr. This domain name is managed by CenpacNet, Nauru's internet service provider. The Uniform Domain Name Dispute Resolution Policy applies.
Consumer protection	*Initial*	The Prices Regulation Act 2008 provides for the regulation of prices of essential goods and services. No other consumer protection legislation identified.

Legal and regulatory frameworks		
Intellectual property legislation	*Initial*	Nauru has a Patents Registration Act 1973 and a Trade Marks Regulations Adoption Ordinance 1964. No legislation providing for copyright protection identified.
Access to information	*Initial*	The Official Information Act 1976 prohibits the unauthorised communication of certain official information. It does not, however, provide for public access to official information.

Recommendations

We have not been able to discuss the matters set out above with Nauru representatives. On the basis of our desktop review, our preliminary recommendations are as follows:

- *Develop a cybersecurity strategy*: Nauru should develop a national cybersecurity strategy, identifying relevant risks, and a plan to strengthen Nauru's cyber framework. The strategy could also identify critical infrastructure, and a system for monitoring and reporting on threats and vulnerabilities. It may be simplest to develop this strategy as part of the development process for a National ICT Policy (if this process is still ongoing).
- *Improving the resourcing and training for cybercrime investigation and prosecution*: Nauru has a strong legislative framework for cybercrime and child protection. To ensure this legislation can be implemented, and cybercrime incidents effectively investigated and prosecuted, Nauru should ensure that adequate resourcing and training is available to law enforcement, prosecutors and the judiciary. We recommend that regional initiatives be funded to train law enforcement, prosecutors and the judiciary to enable small countries like Nauru, with limited resources, to adequately prepare itself for cyber risks.

Niue

Summary

Niue has some law enforcement capability for cybersecurity matters, particularly through the Niue branch of the PTCN and other regional law enforcement cooperation. However, Niue does not presently have any cybersecurity policy or strategy or specific cybersecurity legislation.

Other than intellectual property legislation passed in New Zealand, Niue does not have a substantive legislative framework for safeguarding electronic transactions.

To give a sense of scale, an estimate of the size of the population in Niue is 1,600 people.

Cybersecurity

Strategy and governance		
National cybersecurity strategy	*None*	Niue does not have a published national cybersecurity strategy. A National ICT Strategy was envisaged in the Niue National Strategic Plan 2009-2013, but does not appear to have been finalised. Some ICT-related matters may be covered in the Niue National Strategic Plan 2016-2026.
Governance	*Initial*	The Information Services Office in the Department of Administration has previously been responsible for coordinating ICT policy within the Niue government, including the GON Information Systems Policy and the GON Computer Usage Policy. Responsibilities for ICT in the Niue government now appear to be with the Data and Information Agency. There is no agency with specific responsibility for cybersecurity, although it is likely that these responsibilities would also fall to the Data and Information Agency.
Security		
Institutions	*Initial*	In the event of a cybersecurity incident, the Data and Information Agency and Telecom Niue are likely to be involved in any response effort. Niue does not have a CERT. The Niue branch of the PTCNis the designated agency for the investigation of cybercrime cases.
Critical infrastructure	*None*	No cybersecurity arrangements for critical infrastructure identified.
Vigilance		
Incident reporting	*Initial*	No cybersecurity incident reporting requirements identified.
Domestic cooperation	*None*	No formal domestic cooperation frameworks identified. Cybersecurity matters in Niue are likely to involve the Internet Users Society Niue (an ICANN at-large structure), Telecom Niue, the Niue Police Force and Crown Law. Some cyber awareness programmes are running in schools and the Niue community.

International cooperation	*Initial*	Niue is a member of PaCSON, PICISOC, PICP and PTCN, and is an associate member of APT. Telecom Niue is also a member of PITA. Niue is involved in the Cyber Safety Pasifika programme. Niue is a non-participating country of the PIRRC (receiving indirect benefits) and is among the beneficiaries of the ICB4PAC project. Niue has some international law enforcement links, including to the AFP (with the Pacific Police Development Program) and to the New Zealand Police (with the Pacific Island Prevention Programme). The Mutual Assistance in Criminal Matters Act 1998 and the Extradition Act 1965 provide for mutual assistance and extradition processes.
Resilience		
Cybercrime (substantive)	*None*	Niue does not currently have any specific cybercrime legislation, although a draft cybercrime bill is under preparation by Crown Law. Niue's Constitution notes that Acts of the New Zealand Parliament may apply to Niue where requested and consented to by the Niue Assembly.
Cybercrime (child protection)	*Initial*	No child protection legislation identified, other than an offence for distributing indecent documents in the Niue Act 1966. Niue has acceded to the Convention on the Rights of the Child.
Cybercrime (procedural)	*Initial*	The Niue Act 1966 contains general powers of search and seizure, but no other relevant procedural powers have been identified.
Law enforcement	*Initial*	There are no dedicated cybersecurity Police officers, due to the relatively small size of the Niue Police Force. In the event of a cybercrime incident, the Niue Police Force would look to the PTCN based in Samoa for assistance. The Niue Police Force also has close links with the New Zealand Police and the Australian Federal Police, and could request assistance from contact points in these entities.
Prosecution	*Initial*	We expect prosecution capacity to be low, given the limited cybercrime training for the police and the lack of cybercrime prosecutions, although Niue Crown Law could look to New Zealand for assistance.
Courts	*Initial*	We expect judicial capacity to be low, given the limited cybercrime training for the police and the lack of cybercrime prosecutions.

Safeguarding electronic transactions

Legal and regulatory frameworks		
Electronic transactions	*None*	No general legislation enabling electronic transactions identified. Niue has recently requested that a "Rapid e-Trade Readiness Assessment" be conducted by UNCTAD.

Legal and regulatory frameworks		
Privacy, freedom of speech and other human rights online	*None*	No legislative protection for fundamental human rights or privacy.
Data protection	*None*	No general data protection legislation identified.
Digital authentication	*None*	There is no identity register for individuals in Niue, although a birth register is established under the Births and Deaths Registration Regulations 1984. The Niue National Strategic Plan 2009-2013 envisaged development of an e-government strategy, although this does not appear to have progressed.
ccTLD administration	*Established*	.nu is the TLD assigned to Niue. It is managed by the IUSN Foundation, a non-profit based in Massachusetts, which apparently uses the revenue from the sale of .nu domain names to fund internet services in Niue. The Uniform Domain Name Dispute Resolution Policy applies.
Consumer protection	*Initial*	Some regulation of communications fees in regulations made under the Communications Act 1989. No other consumer protection legislation identified.
Intellectual property legislation	*Established*	Under the version of the Niue Act 1966 (NZ) in force as an enactment of the New Zealand Parliament, the Copyright Act 1994, the Designs Act 1953, the Patent Act 1953 and the Trade Marks Act 2002 (all New Zealand statutes) are in force in Niue. The Copyright Act 1994 includes certain criminal offences relating to copyright infringement.
Access to information	*None*	No general freedom of information legislation identified.

Recommendations

On the basis of our desktop review and discussions with Niue representatives, our recommendations are as follows:

- *Develop cybersecurity strategy*: Niue could consider developing a simple cybersecurity strategy, perhaps as part of the National ICT Strategy that is under-development, to specifically identify key risks and priority actions to strengthen Niue's ability to detect and respond to cyber incidents. The strategy should identify an agency responsible for cybersecurity (presumably the Data and Information Agency), and outline the functions and responsibilities of related agencies.

- *Progress the draft Cybercrime Bill*: Niue should continue development of the draft Cybercrime Bill, drawing on the Budapest Convention as a precedent. Alongside new legislation, it will be important to ensure that the police, prosecutors and the judiciary are adequately resourced and trained to deal with cyber cases. Given the small size of Niue, resourcing should draw on international links, including to Australia and New Zealand.

Palau

Summary

Palau has enacted some legislative provisions addressing substantive cybercrime matters, including child online protection. Palau does not have a published national cybersecurity strategy and does not appear to have designated any institutions as responsible for cybersecurity policy or incident response.

The Palau National Code contains some general provisions relating to safeguarding electronic transactions, data protection, intellectual property and consumer protection.

To give a sense of scale, an estimate of the size of the population in Palau is 22,000 people.

Cybersecurity

Strategy and governance		
National cybersecurity strategy	*None*	No cybersecurity policy or strategy identified.
Governance	*None*	No governance structure for cybersecurity identified. The Office of the Attorney-General has responsibility for prosecuting criminal matters, and the Criminal Investigations Division of the Ministry of Justice has responsibility for investigating criminal matters. Not clear where responsibility for cybersecurity policy would sit (although possibly in the Ministry of Public Infrastructure, Industries and Commerce).
Security		
Institutions	*None*	No specific agency with designated responsibility for cybersecurity policy, and no national CERT or other agency with responsibility for incident response.
Critical infrastructure	*None*	No cybersecurity arrangements for critical infrastructure identified.
Vigilance		
Incident reporting	*Initial*	No cybersecurity incident reporting requirements identified.
Domestic cooperation	*None*	No formal domestic cooperation procedures identified.
International cooperation	*Initial*	Palau is a member of APT, PaCSON, PICISOC, PICP and PTCN. Palau National Communications Corporation is also a member of PITA. Palau has participated in Cyber Safety Pasifika, although we understand cyber awareness remains low and there is a continuing need for awareness-raising programmes. Palau is a non-participating country for the PIRRC (receiving indirect benefits) and is among the beneficiaries of the ICB4PAC project.

		Palau has some international law enforcement links, including to the AFP (with the Pacific Police Development Program). The Palau National Code has provisions for mutual legal assistance and extradition in Titles 17 and 18.
Resilience		
Cybercrime (substantive)	*Initial*	Title 17, chapter 31, of the Palau National Code sets out several cybercrime offences, including computer fraud, computer damage, unauthorised computer access and use of a computer in the commission of a separate crime. Title 17, chapter 31, sets out credit card offences, including an offence for fraudulent use of a credit card.
Cybercrime (child protection)	*Established*	Title 17, chapter 18, of the Palau National Code includes several child exploitation offences including producing, disseminating or possessing child abuse material and exposing children to 'indecent electronic displays'. The offence of use of a computer in the commission of a separate crime, in chapter 31, also includes grooming potential victims of sexual assault, child exploitation and/or child abuse material. Palau has acceded to the Convention on the Rights of the Child.
Cybercrime (procedural)	*Initial*	Provisions in the Palau National Code and Palau Rules of Criminal Procedure provide for general search and seizure powers and the issuing of subpoenas for production of evidence. These provisions do not specifically refer to electronic evidence.
Law enforcement	*Initial*	One officer of the Palau Criminal Investigations Division has received some training in cybersecurity matters in Australia. The general capacity of Palau's law enforcement to deal with cyber matters appears to be low.
Prosecution	*Initial*	We expect prosecution capacity to be low, given the limited cybercrime training for the police and the lack of cybercrime prosecutions.
Courts	*Initial*	We expect judicial capacity to be low, given the limited cybercrime training for the police and the lack of cybercrime prosecutions.

Safeguarding electronic transactions

Legal and regulatory frameworks		
Electronic transactions	*None*	No general legislation enabling electronic transactions identified.
Privacy, freedom of speech and other human rights online	*Initial*	Title 1 (General Provisions) of the Palau National Code provides fora number of human rights under chapter 4 (Trust Territory Bill of Rights), including a right to be secure against unreasonable search and seizure. Privacy rights and online activity are not specifically referred to.

Legal and regulatory frameworks		
Data protection	*Initial*	Title 17 (Crimes) of the Palau National Code contains an offence for unauthorised possession of confidential personal information (including in digital form) in chapter 26. No general privacy or data protection regulation identified.
Digital authentication	*None*	No digital authentication system identified.
ccTLD administration	*Established*	The .pw domain name is managed by the Micronesia Investment & Development Corporation. It is an open ccTLD, and has been rebranded as the Professional Web. The Uniform Domain Name Dispute Resolution Policy applies to .pw domains.
Consumer protection	*Established*	Title 11 (Business and Business Regulation) of the Palau National Code contains various provisions for consumer protection, including regulation of unfair business practices. A specific Consumer Protection Act is set out in chapter 2 of Title 11, covering misleading and deceptive conduct and other prohibited acts.
Intellectual property legislation	*Established*	Title 39 (Real and Personal Property) of the Palau National Code contains various provisions relating to copyright and performers' rights in chapter 8. These provisions include offences for infringement of copyright and performers' rights, which could apply to infringement online.
Access to information	*Established*	Palau's Open Government Act, enacted in 2014, provides for open and transparent government, including procedures for access to public records and government documents.

Recommendations

On the basis of the desktop review and discussions with Palau representatives, our recommendations are as follows:

- *Develop cybersecurity strategy*: Palau should develop a cybersecurity policy and/or strategy document, to specifically identify key risks and priority actions to strengthen Palau's ability to detect and respond to cyber incidents. The strategy should identify an agency responsible for cybersecurity, and outline the functions and responsibilities of related agencies.
- *Strengthen cybercrime framework*: Palau has criminalised certain cybercrime offences, but has not adopted the Budapest Convention framework. It may be worth developing a more comprehensive cybercrime framework, including specific procedural rules as necessary to enable the effective prosecution of cybercrimes. In parallel, it is important to ensure that adequate resourcing and training is provided to law enforcement, prosecutors and the judiciary so that all are well-equipped to deal with cyber cases.

- *Legislative support for a digital economy*: Palau has legislation addressing consumer protection, copyright infringement and open government, but does not have laws providing for the equivalency and legal validity of electronic transactions and for the regulation of collection, use and disclosure of personal information. Palau should keep these laws on the agenda while it focusses on cybersecurity, for when the reform capacity is available and there is a need to support the use of technology and electronic transactions by its citizens.

Papua New Guinea

Summary

Papua New Guinea developed a National Cybersecurity Policy in 2014. This policy sets out the roles of various government stakeholders in combating cybercrime and describes the priority areas for government action going forward.

In accordance with the National Cybersecurity Policy, Papua New Guinea enacted comprehensive cybercrime legislation in 2016. Following the enactment of this legislation, a key area of focus is increasing the capacity of the criminal justice system to investigate and prosecute cybercrimes. Papua New Guinea also recently established a CERT, in January 2018.

We understand that specific legislation relating electronic transactions is in the process of development, which will complement other related legal frameworks already in place in Papua New Guinea.

To give a sense of scale, an estimate of the size of the population in Papua New Guinea is 8,418,300 people.

Cybersecurity

Strategy and governance		
National cybersecurity strategy	*Established*	Papua New Guinea has a National Cybersecurity Policy, finalised in July 2014. A National Cybersecurity Strategy, to complement the 2014 policy, is currently under development.
Governance	*Established*	The National Information and Communication Technology Authority (*NICTA*) regulates the ICT industry and has primary responsibility for cybersecurity policy. The Department of Justice and the Attorney General is responsible for international cooperation on cybercrime matters, and for the continuing development of cybercrime legislation. The Department of Communication and Information (*DCI*) is responsible for the administration of government policies on ICT matters, including cybercrime policies. The Royal Papua New Guinea Constabulary is a law enforcement agency, and has responsibility for the enforcement of cybercrime legislation. The Office of the Public Prosecutor has responsibility for prosecuting cybercrime offences. The Department of Prime Minister and NEC assists on cybercrime matters as they relate to the sovereignty, unity and security of Papua New Guinea.
Security		
Institutions	*Established*	As noted above, NICTA is the institution responsible for implementing national cybersecurity policy in Papua New Guinea.

		Papua New Guinea established a national CERT in January 2018 (*PNGCERT*). PNGCERT is intended to coordinate the response to national cybersecurity incidents, promote cybersecurity situational awareness, advocate for capacity building, coordinate with international counterparts and promote secure systems and networks within Papua New Guinea. APNIC was involved in the establishment of PNGCERT.
Critical infrastructure	*None*	No cybersecurity arrangements for critical infrastructure identified, although this area would appear to be part of the mandate of PNGCERT.
Vigilance		
Incident reporting	*Initial*	Some cybercrime reporting occurs, generally to the police. No mandatory reporting requirements identified.
Domestic cooperation	*Initial*	The National Cybersecurity Policy recognises the importance of cross-agency collaboration and sharing of information in combatting cybercrime. No formal collaboration arrangements identified.
International cooperation	*Initial*	The National Cybersecurity Policy recognises the importance of international collaboration in combatting cybercrime. Papua New Guinea is a member of APT, CTO, Interpol, ITU-IMPACT initiative, PacSON, PICISOC, PICP, PITA and PTCN. Papua New Guinea is also a participating country for the PIRRC and is among the beneficiaries of the ICB4PAC project (not including in-country technical assistance). Papua New Guinea police have a direct cooperation programme with the AFP. The Cybercrime Code Act 2016 confirms that the Mutual Assistance in Criminal Matters Act 2005 and the Extradition Act 2005 apply to cybercrime offences.
Resilience		
Cybercrime (substantive)	*Sophisticated*	The Cybercrime Code Act 2016 provides for a comprehensive set of cybercrime offences, drawing on the Budapest Convention and other precedents. This Act also criminalises data espionage, defamatory publications, cyber bullying, cyber harassment, unlawful disclosure of information, spam emails and intellectual property infringement. The inclusion of this broad range of offences has generated some concern about the potential for this Act to be used to restrict legitimate criticism of the Papua New Guinea government and other free expression.
Cybercrime (child protection)	*Established*	The Cybercrime Code Act 2016 sets out offences for child abuse material and child online grooming. Sections 229C and 229R-T of the Criminal Code also set out offences against children which could occur online, including

		indecent acts directed at a child, and various child abuse material offences. Papua New Guinea has signed and ratified the Convention on the Rights of a Child.
Cybercrime (procedural)	*Sophisticated*	The Cybercrime Code Act 2016 sets out procedural powers intended to assist with the investigation and prosecution of cybercrime, including powers relating to search and seizure, preservation of evidence and collection of traffic data.
Law enforcement	*Initial*	The National Cybersecurity Policy emphasises the importance of investing in law enforcement agencies to effectively combat cybercrime, and specifically discusses the establishment of a Cybercrime Investigative Unit within the police force. It is not clear whether this unit is currently established. We understand that the capacity of law enforcement to investigate cybercrime in Papua New Guinea is low, and that this lack of capacity may be inhibiting prosecutions under the Cybercrime Code Act 2016. To date, there have been no convictions under this Act, although some charges have been laid.
Prosecution	*Initial*	We expect prosecution capacity to be low, given the limited cybercrime training for the police and the lack of cybercrime prosecutions.
Courts	*Initial*	We expect judicial capacity to be low, given the limited cybercrime training for the police and the lack of cybercrime prosecutions.

Safeguarding electronic transactions

Legal and regulatory frameworks		
Electronic transactions	*None*	An Electronic Transactions Act, drawing on the UNCITRAL model laws, is in the process of development.
Privacy, freedom of speech and other human rights online	*Initial*	Section 49 of the Constitution of Papua New Guinea sets out a right to reasonable privacy in respect of private and family lives, communications with other people, and personal papers and effects. The Protection of Private Communications Act 1973 provides protection for private communications and defines the circumstances in which private communications may be intercepted and the use that can be made of that information. No specific protections for the exercise of human rights online have been identified.
Data protection	*Initial*	The Cybercrime Code Act 2016 makes unlawful disclosure of electronic information an offence.

Legal and regulatory frameworks		
		No overarching privacy or data protection legislation, although we understand preparation of this type of legislation is under consideration by the Papua New Guinea government.
Digital authentication	*Initial*	The Papua New Guinea National Identification card system was introduced in 2016. Current estimates suggest 500,000 of Papua New Guinea's approximately 8 million people are registered in this system. It does not appear that use of this system extends to digital authentication.
ccTLD administration	*Initial*	The .pg domain name is administered by the Papua New Guinea University of Technology. No dispute resolution policies identified.
Consumer protection	*Established*	The Independent Consumer and Competition Commission (the *ICCC*) in Papua New Guinea has a consumer protection division. The ICCC is responsible for enforcing the Commercial Advertisement (Protection of the Public) Act. The Cybercrime Code Act 2016 also includes an offence for unlawful advertising.
Intellectual property legislation	*Established*	Sections 28-30 of the Cybercrime Code Act 2016 criminalise online intellectual property infringement, including online copyright infringement, online sale of goods to which a forgery of a trademark is applied, and online contravention of patent law.
Access to information	*None*	Section 46 of the Constitution of Papua New Guinea sets out a right to freedom of expression and publication, which includes the right to receive ideas and information and to communicate ideas and information. No legislation providing for access to public information identified.

Recommendations

On the basis of the desktop review and discussions with Papua New Guinea representatives, our recommendations are as follows:

- *Continued implementation and update of National Cybersecurity Policy*: Papua New Guinea's cybersecurity strategy is relatively well developed, with the formulation of the National Cybersecurity Policy, enactment of the Cybercrime Code Act 2016 and the recent creation of PNGCERT. We suggest updating this policy to reflect these developments, and to identify areas of focus for the next 5 to 10 years, perhaps as part of the current development of a National Cybersecurity Strategy. These areas might include implementing rules or policies relating to critical infrastructure and incident reporting.
- *Capacity improvements*: Papua New Guinea should focus on improving the capacity of incident response, law enforcement, prosecution and judicial agencies so that cybercrime can be effectively detected, reported and prosecuted. In parallel, it is important to improve public awareness of cybercrime and cybersecurity matters, so that citizens know what to do to protect themselves, drawing perhaps on the Cyber Safety Pasifika programme.
- *Legislative support for a digital economy*: Papua New Guinea should continue the development of electronic transactions legislation, and should commence development of privacy and data protection legislation,

regulating the collection, use and disclosure of personal information. Development of these laws will support the increasing use of technology and electronic transactions by citizens in Papua New Guinea.

Republic of the Marshall Islands

Summary

The Republic of the Marshall Islands (*RMI*) does not have a national cybersecurity strategy, although the Ministry of Transportation, Communication and Information Technology has some responsibility for cybersecurity policy.

RMI has some legislative offences relating to cybercrime and child protection matters. However, capacity for enforcing cybercrime offences is low.

A Computer Crimes Bill was developed in 2011 but this has not progressed. RMI also has some legislative frameworks for safeguarding electronic transactions, particularly relative to consumer protection and intellectual property. However, RMI has no directly enabling legislation for electronic transactions and has not enacted any privacy or data protection frameworks.

To give a sense of scale, an estimate of the size of the population in the Marshall Islands is 53,200 people.

Cybersecurity

Strategy and governance		
National cybersecurity strategy	*Initial*	RMI does not have a published national cybersecurity strategy. RMI does have a National ICT Policy, produced in 2012, and ICT matters feature in the National Strategic Plan 2015-2017.
Governance	*Established*	The Ministry of Transport, Communications and Information Technology has responsibility for ICT, and may also have responsibility for cybersecurity matters. The National Telecommunications Authority, a majority government-owned company, is responsible for the provision of telephone and internet services in RMI, including ICT support. Other stakeholders include the Office of the Attorney-General, the Office of the Auditor-General and the RMI Police Force.
Security		
Institutions	*Initial*	As above, the Ministry of Transport, Communications and Information Technology appears to have the closest existing mandate, with responsibility for ICT. RMI does not have a CERT.
Critical infrastructure	*None*	No cybersecurity arrangements for critical infrastructure identified.
Vigilance		
Incident reporting	*None*	No cybersecurity incident reporting requirements identified. Awareness training was identified as a priority by many stakeholders – RMI Police, Ministry of Education, Auditor General's Office, NTA.

		The RMI Police and the National Telecommunications Authority are in discussions about conducting further awareness-raising exercises before the introduction of 4G technology.
Domestic cooperation	*None*	No formal domestic cooperation arrangements identified.
International cooperation	*Initial*	The RMI is a member of APT, Interpol, ITU-IMPACT initiative, PaCSON, PICISOC, PICP, PITA and PTCN. RMI is also a participating country for the PIRRC and is among the beneficiaries of the ICB4PAC project. Representatives from the RMI Police attend AFP workshops/training. However, the Cyber Pasifika programme has not been implemented on the ground. RMI law enforcement tends to look to the US for assistance when required, particularly through the FBI in Guam and Hawaii. Links with AFP (with the Pacific Police Development Program) and New Zealand law enforcement exist, but are less well-established. The Mutual Assistance in Criminal Matters Act 2002 provides for mutual legal assistance in criminal matters, for offences with a maximum penalty of at least one year's imprisonment. The Criminal Extradition Act (Title 32 of the Marshall Islands Revised Code) sets out rules and procedures for extradition for all criminal offences.
Resilience		
Cybercrime (substantive)	*Initial*	The Criminal Code 2011, article 250 criminalises harassment and, under the heading of "violation of privacy", surveillance and interception of private communications. Harassment includes repeatedly making electronic mail transmissions without "a purpose of legitimate communication". Article 224 sets out offences for forgery and other fraudulent practices. The Counter-Terrorism Act 2002, s 105(38)(g) provides that any act designed to disrupt or destroy an electronic system, where intended to intimidate the public or compel a government or organisation to act or refrain from acting, will be considered a terrorist act.
Cybercrime (child protection)	*Initial*	The Criminal Code 2011, article 230, criminalises child abuse and neglect, endangering the welfare of children, and trafficking in children. RMI has signed and ratified the Convention on the Rights of the Child, which is implemented by the Child Rights Protection Act 2015, including matters relating to child abuse material. The Child Abuse and Neglect Act 2016, s502(2) includes within the definition of child abuse, physical harms, sexual exploitation and "injury to the psychological capacity of the child." This could potentially extend to bullying. No explicit reference is made to offences committed online or through a computer.

Cybercrime (procedural)	*Initial*	The Criminal Procedure Act, Part III provides for general search and seizure powers.
Law enforcement	*Initial*	Low capacity, although RMI law enforcement does have the ability to request assistance from the FBI, AFP and New Zealand Police as necessary. The Office of the Auditor General employs a forensic auditor, with experience in digital forensics.
Prosecution	*Initial*	We expect prosecution capacity to be low, given the limited cybercrime training for the police and the lack of cybercrime prosecutions.
Courts	*Initial*	We expect judicial capacity to be low, given the limited cybercrime training for the police and the lack of cybercrime prosecutions.

Safeguarding electronic transactions

Legal and regulatory frameworks		
Electronic transactions	*None*	No general enabling legislation for electronic transactions identified.
Privacy, freedom of speech and other human rights online	*Established*	The Constitution of the Republic of the Marshall Islands, article 2, includes the rights to freedom of thought, freedom of speech, freedom of association and freedom from unreasonable intrusions into privacy. As noted above, the Criminal Code 2011 includes offences relating to violation of privacy, including unlawful surveillance and interception of private messages. The Child Rights Protection Act 2015 provides that no child shall be subjected to arbitrary or unlawful interference with his/her privacy.
Data protection	*Initial*	No general privacy or data protection legislation identified. Persons employed in the performance of functions under the Statistics Act 1986 commit an offence if they improperly disclose any information acquired in the course of their employment. Similarly, there is a secrecy requirement for employees working for the Marshall Islands Social Security Administration under the Social Security Act 1990.
Digital authentication	*Initial*	Under the Registration of Persons Act 1979, every citizen of the Marshall Islands is eligible to be registered in the Register of Persons. Registered Persons are eligible to receive an identity card, a social security number and a tax identification number. The national identity card scheme is used to prove the identity of citizens when opening bank account, etc., but does not yet have a digital authentication feature.

Legal and regulatory frameworks		
ccTLD administration	*Initial*	The ccTLD for the Marshall Islands is .mh, but does not appear to be active. The Office of the Cabinet is listed as the ccTLD manager. We understand that most websites related to the Marshall Islands are hosted in other countries. No dispute resolution procedures appear to apply.
Consumer protection	*Established*	The Consumer Protection Act 2004 prohibits unfair and deceptive acts or practices in trade. Lessening of market competition is regulated by the Unfair Business Practices Act.
Intellectual property legislation	*Initial*	The Unauthorised Copies of Recorded Materials Act 1991 protects sound recordings and audio-visual works from being copied without authorisation. It does not have explicit application online.
Access to information	*Initial*	The Marshall Islands Administrative Procedure Act 1979, s 103 requires each agency to make available for public inspection all rules and all other written statements of policy or interpretations used by the agency, together with all final orders, decisions and opinions of general applicability or effect on the public.

Recommendations

On the basis of our desktop review and discussions with stakeholders during our visit to the Republic of the Marshall Islands, our recommendations are as follows:

- *Develop a cybersecurity strategy*: RMI should develop a national cybersecurity strategy, identifying relevant risks, and a plan to strengthen RMI's cyber framework. The strategy could also assign roles and responsibilities to relevant agencies. It may be simplest to develop this strategy as part of a revised National ICT Policy or during an update to the National Strategic Plan. RMI stakeholders prefer that cybersecurity be included in the National Strategic Plan and be linked to Strategic Development Goals.
- *Strengthen cybercrime framework:* While there are some cybercrime provisions in place in RMI legislation, these provisions may not be sufficiently specific to enable prosecution of the full range of cyber-criminal activities. RMI should develop a new cybercrime statute, drawing on the Budapest Convention and reflecting the specific circumstances of RMI. RMI stakeholders support the development of a Pacific standard for this legislation.
- *Capacity building:* RMI should improve capacity for responding to cybercrime, by providing training to relevant stakeholders, including investigators, prosecutors and the judiciary. RMI stakeholders prefer hands on training, such as secondments.
- *Public awareness initiatives*: police officers in RMI are aware of Cyber Pasifika but the programme is not yet not implemented in country.
- *Developing a legislative framework for a digital economy*: RMI has an established consumer protection framework and has constitutional privacy rights, but otherwise has a relatively undeveloped legal framework to support e-commerce. Development of this framework should remain on the agenda while

cybersecurity is progressed, for when the reform capacity is available and the need identified to support the increasing use of technology and electronic transactions by RMI citizens.

Samoa

Summary

Samoa has a relatively well-developed legal and regulatory framework for cybersecurity and electronic transactions. In particular, Samoa has established a national authority for cybersecurity, the National ICT Steering Committee, and has designated the various organisations that have roles important for cybersecurity.

Samoa has also developed a five-year cybersecurity strategy (from 2016 to 2021), outlining Samoa's intended direction for cybersecurity legislation and governance over that time.

We understand from the Attorney General's office that it has instructions from the Prime Minister to commence the ratification process to accede to the Budapest Convention. The Attorney General's office, stakeholders and representatives from the Council of Europe met during 2018 to build capacity, conduct a gap analysis and form recommendations for bridging the gap between Samoa's current legal and regulatory framework and Budapest Convention standards.

Following Budapest Convention ratification, Samoa's primary areas of focus include building capacity for investigation and prosecution of cybercrime offences and developing privacy and data protection legislation.

To give a sense of scale, an estimate of the size of the population in Samoa is 197,700 people.

Cybersecurity

Strategy and governance		
National cybersecurity strategy	*Established*	Samoa National Cybersecurity Strategy: 2016-2021.
Governance	*Established*	The Ministry of Communication and Information Technology (*MCIT*) is the governing authority for all ICT and cybersecurity-related matters. It is responsible for setting cybersecurity policy, coordinating reviews of legislation and prescribing powers for law enforcement agencies to combat cyber threats. The MCIT works with the Office of the Regulator (*OOTR*) and the Attorney General's office, to develop and review legislation pertaining to cybersecurity.
Security		
Institutions	*Established*	The National ICT Steering Committee (*NICT*) is responsible for the implementation of the cybersecurity strategy. It is the national competent authority on the security of network and information systems. The NICT will coordinate the National Crime Prevention Strategy related to Cybercrime in conjunction with the National Prosecution Office, the Judiciary and law enforcement agencies. As a continuation of the 2016 cybersecurity project, ITU and DFAT engaged Oxford and Australian cybersecurity experts to conduct

		assessments of Samoa's capacity and readiness. The report from those assessments is scheduled for release and will provide guidance as to how to form its CERT. Part of that project will also identify where Samoa can access assistance to establish a CERT, as the knowledge, capacity and skills are not readily available in Samoa.
Critical infrastructure	*Initial*	The Samoa National Broadband Highway Project has the potential to provide a full scale national broadband infrastructure to connect all the government ministries and their agents. We understand there have been challenges in utilising the infrastructure. No cybersecurity requirements for critical infrastructure identified.
Vigilance		
Incident reporting	*None*	No cybersecurity incident reporting requirements identified.
Domestic cooperation	*Established*	Samoa's cybersecurity strategy provides that MCIT governs the NICT, which in turn coordinates all strategies related to cybersecurity. The Office of the Attorney General, Samoan Law Reform Commission and National Prosecution Office cooperate with law enforcement to develop the National Crime Prevention Strategy. The MCIT, OOTR and Samoan Qualification Authority are expected to develop a framework for the certification and accreditation of national agencies and public sector organisations by internationally recognised cybersecurity standards.
International cooperation	*Initial*	Samoa is a member of APT, CTO, Interpol, ITU-IMPACT initiative, PaCSON, PICISOC, PICP, PITA and PTCN (with the Pacific Transnational Crime Coordination Centre located in Apia, Samoa). Samoa is a participating country for the PIRRC and is among the beneficiaries of the ICB4PAC project. Samoa is also a participant in Cyber Safety Pasifika. Samoa has some international law enforcement links, including to the AFP (direct cooperation programme) and to the New Zealand Police (with the Pacific Island Prevention Programme). The Mutual Assistance in Criminal Matter Act 2007 and Extradition Act 1974 provide for mutual assistance and extradition processes.
Resilience		
Cybercrime (substantive)	*Established*	The: • Crimes Act 2013, Part 18 (offences relating to accessing electronic systems, illegal remaining, and damaging, interfering with or intercepting data); and • Telecommunications Act 2005, s 74 (offences relating to accessing, intercepting or altering data, and hindering or

		inappropriately using a telecommunications network), contain explicit cybercrime offences and cyber enabled-offences. While the Attorney General's Office gaps analysis identified that the existing Crimes Act already provides for cybercrime offences in line with the Budapest Convention, we understand a policy decision has been made to have a standalone cybercrimes law. On that front, preliminary work is underway to develop comprehensive cybercrime legislation, alongside Budapest Convention ratification preparation.
Cybercrime (child protection)	*Established*	The: • Crimes Act 2013, Part 18 (solicitation of children through technology); and • Family Safety Act 2013 (applications for protection orders and offences for breaching protection orders), contain child protection provisions. Samoa has signed and ratified the Convention on the Rights of the Child and has acceded to the Optional Protocol on the Sale of Children, Child Prostitution and Child Pornography.
Cybercrime (procedural)	*Initial*	Relevant procedural rules appear in Criminal Procedure Act 2016, s 33 (not limited to physical evidence); Police Powers Act 2007, s 32 (powers for police to seize evidential material while executing a search). There is no legislation specifically relating to the preservation of electronic data. We understand from MCIT that the Ministry of Police is keen to see specific cybercrime legislation developed as while the Crimes Act sets out various cyber offences, the law falls short on adequate procedural and assistance requirements for effectively prosecuting cybercrimes.
Law enforcement	*Initial*	There is a single point of contact for cybercrime within the Ministry of Police. The cybersecurity strategy envisages that a sustainable training program will be developed for law enforcement officers.
Prosecution	*Initial*	The cybersecurity strategy envisages that a sustainable training program will be developed for prosecutors. Prosecution capacity is low, given the limited cybercrime training available to the police to date. Education and awareness training for prosecutors, as well as judges and legal practitioners, was identified by almost all stakeholders as a key priority.
Courts	*Initial*	The cybersecurity strategy envisages that a sustainable training program will be developed for the judiciary. Judicial capacity is low, given the limited cybercrime training available. Education and awareness training for judges, as well as prosecutors and legal practitioners, was identified by almost all stakeholders as a key priority.

Safeguarding electronic transactions

Legal and regulatory frameworks		
Electronic transactions	*Established*	The Electronic Transactions Act 2008 makes provision for e-signatures and electronic contracts, drawing on the UNCITRAL model laws. The National Payment System Act refers to online transactions. UNCTAD completed a "Rapid e-Trade Readiness Assessment" for Samoa in 2017.
Privacy, freedom of speech and other human rights online	*Initial*	Freedom of speech is protected in the Constitution of the Independent State of Samoa, s 13(a).
Data protection	*Initial*	Several statutes protect the privacy of individuals' data in particular contexts, such as the Broadcasting Act 2010, ss 44-45; and the Births, Deaths and Marriages Registration Act 2002, s 75. Use of data collected by ISPs is governed by the Telecommunications Act 2005, s 50. There is no overarching privacy or data protection framework.
Digital authentication	*Initial*	A register of citizens' identities is mandated by the Births, Deaths and Marriages Registration Act 2002. MCIT is considering how a system for digital identification could be developed, and whether blockchain technology may provide a solution. The Office of the Electoral Commission are investigating biometric scanning for voting purposes, which may develop into a broader authentication project.
ccTLD administration	*Established*	.ws is the ccTLD for Samoa. It is administered by Samoa NIC on behalf of the Ministry of Foreign Affairs for the government of Samoa. The government has oversight of a register of sub-domains including "gov.ws" and "edu.ws". The Uniform Domain Name Dispute Resolution Policy applies.
Consumer protection	*Established*	Fair Trading Act 1998; Competition and Consumer Act 2016.
Intellectual property legislation	*Established*	Copyright Act 1998 (technology neutral), including an offence for copyright infringement. Intellectual Property Act covers trade marks and domain names and is also technology neutral.
Access to information	*Initial*	The Public Records Act 2011, s 27 provides that a public record may be made accessible to the public once 25 years have elapsed since it came into existence. The Authority can direct that a Public Record be withheld (s 30). The Constitution, s 82A establishes the Office of the Ombudsman. There are however no explicit powers to require disclosure of public information.

Legal and regulatory frameworks		
		The Samoan Law Reform Commission self-initiated a review of the framework for sharing official information between government departments. A discussion paper proposing a legislative framework for official information sharing is now with Cabinet. The discussion paper does not consider public accessibility of official information.

Recommendations

On the basis of our desktop review and consultation mission to Samoa, our recommendations, in addition to the regional level recommendations, are as follows:

- *Cyber strategy*: Samoa's cybersecurity strategy is relatively well developed. However, MCIT has not yet been able to implement the strategy in a consistent manner due to a lack of awareness and urgency among other stakeholders and parts of government. Implementing the cyber strategy should remain a focus for Samoa, and will be assisted by capacity building at all levels, and cyber awareness. Effective implementation of the cyber strategy may also require focussing on whether additional laws in addition to cybercrime laws should be considered, including laws allowing (or requiring) ISPs to monitor and filter online traffic.
- *Strengthening Samoa's cybercrime framework*: Samoa has some cybercrime provisions in place in its Crimes Act. We understand that MCIT prefers developing and implementing a standalone and comprehensive cybercrimes law, and a gaps analysis is in the process of being finalised through 2018. We recommend that the cybercrime framework be comprehensive, and cover procedural matters to enable effective prosecution. In particular, processes around digital evidence and assistance should be developed and included in any resulting legislation.
- *Digital economy framework*: Samoa has comprehensive consumer protection laws and e-transaction legislation in place, but does not appear to have an overarching privacy or data protection framework. While we do not recommend a data protection framework similar to New Zealand or Australia, we do recommend that MCIT consider how rules governing the use, collection and disclosure of personal information in Samoa could be worked into Samoa's legal framework to provide individuals with a legislative basis for privacy.

Solomon Islands

Summary

The Solomon Islands has no designated cybersecurity legislation, but there are some cyber-related offences in the Telecommunications Act and Criminal Procedure Code. The Solomon Islands has no published national strategy on cybersecurity, and there are no designated institutions responsible for cybersecurity matters, although many institutions are involved in cybersecurity matters.

There is no legislation in place at present to enable e-transactions, or to regulate privacy, data protection or consumer protection.

There is a lot of attention on cyber in the Solomon Islands, but the expertise and interest is spread thinly across different institutions. As with all our in-country consultations, capacity building and retaining local expertise were identified by all stakeholders as key challenges to addressing cyber risk.

To give a sense of scale, an estimate of the size of the population in the Solomon Islands is 623,300 people.

Cybersecurity

Strategy and governance		
National cybersecurity strategy	*None*	No national or sector specific strategy on cybersecurity, although the Solomon Islands does have a National Development Strategy and a National Infrastructure Investment Plan. Cyber is mentioned within the 2017 National ICT Policy.
Governance	*None*	No Ministry or agency with overall responsibility for cybersecurity. Responsibility for ICT policy rests with the Ministry of Communications and Aviation (*MCA*) and responsibility for management of ICT systems and networks rests with the Ministry of Finance.
Security		
Institutions	*None*	The Solomon Islands has no national CERT or cybersecurity-focussed institution. MCA, the SIG ICT Support Unit (a division of the Ministry of Finance and Treasury), the Telecommunications Commissioner of Solomon Islands and the Information Technology Society Solomon Islands (*ITSSI*) are all involved in cyber-related matters to a degree. ITSSI has been running Government-focussed workshops and awareness campaigns on cyber issues.
Critical infrastructure	*None*	There are no formal or informal cybersecurity arrangements for critical infrastructure.
Vigilance		
Incident reporting	*Initial*	The Solomon Islands has no cybersecurity incident reporting requirements.
Domestic cooperation	*None*	There are no formal or official domestic co-operation protocols. The ICT Society of the Solomon Islands partners with Government on IT issues including security. This society was launched in 2016 and is an association of IT professionals in both public and private sectors.

International cooperation	*Initial*	The Solomon Islands is a member of APT, CTO, Interpol, PaCSON, PICISOC, PICP, PITA and PTCN. The Solomon Islands is a participating country for the PIRRC and is among the beneficiaries of the ICB4PAC project. The Solomon Islands participates in the Cyber Safety Pasifika programme. The Solomon Islands has some international law enforcement links, including a direct cooperation programme with the AFP. The Extradition Act 2010 and Mutual Assistance in Criminal Matters Act 2002 enable international co-operation in certain circumstances, and may facilitate cooperation in response to a cyber-attack.
Resilience		
Cybercrime (substantive)	*Initial*	The Solomon Islands has no designated cybercrime legislation. The Telecommunications Act 2009 contains some offences relevant to cybersecurity, including infringing security to obtain data, intercepting messages, altering/destroying/deleting data, revealing contents of messages, impeding or delaying messages, and possessing a device to do any of the above.
Cybercrime (child protection)	*None*	There is no domestic legislation on child protection online. The Solomon Islands has acceded to the Convention on the Rights of the Child and has signed the Optional Protocol on the Sale of Children, Child Prostitution and Child Pornography.
Cybercrime (procedural)	*Initial*	The general search and seizure powers under the Criminal Procedure Code extend to electronic evidence.
Law enforcement	*Initial*	No designated law enforcement body for cybercrime offences.
Prosecution	*Initial*	Prosecution capacity in the Solomon Islands is low, given the limited cybercrime training for the police. The Solomon Islands Police would look to the AFP for assistance in cyber issues.
Courts	*Initial*	Judicial capacity in the Solomon Islands is low, given the limited cybercrime training available.

Safeguarding electronic transactions

Legal and regulatory frameworks		
Electronic transactions	*None*	No general enabling legislation for electronic transactions identified. UNCTAD completed a "Rapid e-Trade Readiness Assessment" for the Solomon Islands in 2018 but the results of that assessment have not yet been circulated.
Privacy, freedom of speech and other human rights online	*Initial*	There is no specific privacy, freedom of speech or human rights legislation. The right to freedom of expression is enshrined in the constitution and could apply to online communications.

Legal and regulatory frameworks		
Data protection	*None*	The Solomon Islands has no general privacy or data protection legislation.
Digital authentication	*None*	There is no digital authentication system in the Solomon Islands. The Government has identified a need for national ID system but no institution is driving it. Getting correct information is a challenge.
ccTLD administration	*Initial*	The .sb domain name is administered by the Solomon Telekom Company Limited. There are no formal dispute resolution procedures.
Consumer protection	*Initial*	The Telecommunications Act ensures that telecommunications services are provided equitably. No other consumer protection legislation has been enacted.
Intellectual property legislation	*None*	The Solomon Islands has a Copyright Act, a Patents and Trade Marks Act and Cultural IP legislation. However, this legislation is not at an international treaty standard.
Access to information	*None*	There is no access to information legislation and a concern to preserve, for example, Cabinet confidentiality.

Recommendations

On the basis of our desktop review and consultation mission to the Solomon Islands, our recommendations are as follows, to be read alongside the regional recommendations:

- *Developing a coherent cybersecurity strategy and policy:* most stakeholders articulated a lack of coherent policy and "joined up" coordination between institutions as a barrier to making progress on cyber and digital issues. The Solomon Islands would benefit from guidance from countries who have implemented clear cyber strategies and policies, together with capacity building support to implement and execute those policies and strategy. In particular, a cyber-strategy could outline the country's risk profile, given the coming cable connections expected to land in the Solomon Islands over the next 2 – 5 years.
- *Strengthening cybercrime framework*: in conjunction with developing a cyber-strategy, the Solomon Islands would benefit from developing a cybercrime framework of legislation, backed by processes and assistance protocols and supported by training and capacity building.
- *Digital economy framework*: Solomon Islands does not presently have legislation governing electronic transactions, privacy and data protection. While cybersecurity remains a first priority, as the country moves into a new digital era with submarine cable connections, we recommend the Government examine where there is a need and capacity to bolster its existing legislative framework to support a more digital economy.

Tonga

Summary

Tonga's cybersecurity legislative framework is one of the most well developed in the Pacific. The Computer Crimes Act 2003 contains substantive offences such as interfering with and illegally accessing a computer system. This Act also provides procedural powers, such as intercepting electronic communications. The Telecommunications Act 2015 also provides for filtering and take down processes, one of the few Pacific Islands countries to do so.

Tonga's accession to the Budapest Convention in 2017 has given it the impetus, and the resources, to modernise and develop its cybercrime laws further. A draft Computer Crimes Bill has been developed and is in the legislative process. It will repeal and replace the existing Act of the same name. The Bill will enact requirements for Budapest Convention compliance. We understand that following the Computer Crimes Bill, a broader cyber and electronic transactions legislation programme is set to follow.

Tonga has a CERT which is responsible, among other things, for responding to cyber incidents. The CERT is both a hub for communication between key stakeholders (Attorney General's office, Police, Director of Public Prosecutions, MEIDECC, ISPs, critical infrastructure providers), and provides the resources to support Tonga's institutions with cyber issues and investigations.

While there are currently no electronic transaction laws, or overarching privacy or data protection framework, the Attorney General's office and MEIDECC plan for these developments to follow implementation of the Computer Crimes Bill, as part of a broader cybersecurity strategy.

As with most Pacific Island countries, we observe that the pace of development in cybersecurity and electronic transactions is almost wholly dependent on current political will and interest. Where a Minister is particularly interested or aware of digital issues, then the pace of change is quicker. Without Ministerial endorsement, development of legislative and regulatory frameworks in this area will stall, given competing priorities for resources.

To give a sense of scale, an estimate of the size of the population in the Kingdom of Tonga is 109,000 people.

Cybersecurity

Strategy and governance		
National cybersecurity strategy	*Initial*	There is no current national cybersecurity strategy. The Cyber Challenge Task Force, established on 13 December 2013, has been reconstituted as the Cyber Taskforce following Tonga's accession to the Budapest Convention and establishment of a CERT. Once the Computer Crimes Bill is passed, MEIDECC or the Attorney General's office will take the lead in developing a national cybersecurity strategy covering the various areas serviced by the taskforce.
Governance	*Established*	The Cyber Challenge Task Force is the officially recognized agency responsible for implementing a national cybersecurity strategy, policy and roadmap. MEIDECC also has general responsibility for information technology matters.
Security		
Institutions	*Established*	The responsible Ministry is MEIDECC. Tonga has a national CERT.

Critical infrastructure	*Established*	Tonga National CERT is responsible for critical infrastructure, and works in partnership with CERT Australia.
Vigilance		
Incident reporting	*Initial*	Reporting is not mandatory, but CERT has functionality on its website to make a voluntary report.
Domestic cooperation	*Initial*	While no formal domestic cooperation framework exists, domestic cooperation coalesces around the CERT and its role in capacity building, safety, crime and security.
International cooperation	*Established*	The Tonga National CERT works in partnership with CERT Australia, CERT New Zealand and with APNIC. Tonga is a member of APT, CTO, Interpol, PaCSON, PICISOC, PICP, PITA and PTCN. Tonga is a participating country in PIRRC and is among the beneficiaries of the ICB4PAC project. Tonga is a participant in the Cyber Safety Pasifika programme. Tonga has some international law enforcement links, including a direct cooperation programme with the AFP. The Extradition Act provides for computer crime related extradition. Tonga also has a Mutual Assistance in Criminal Matters Act.
Resilience		
Cybercrime (substantive)	*Established*	Computer Crimes Act 2003 criminalises illegal access, interfering with a computer system, illegal devices. Evidence Act allows for the admissibility of electronic evidence in legal proceedings. Tonga acceded to the Budapest Convention in May 2017, becoming the first Pacific Islands nation to do so. A new Computer Crimes Bill has been developed as part of the Budapest Convention accession process, and is in the legislative process. Criminal Offences Act provides for generic fraud.
Cybercrime (child protection)	*Established*	All pornography is prohibited by the Pornography Control Act of 2002. Child abuse material is prohibited in the Criminal Offences Act. Tonga has acceded to the Convention on the Rights of the Child.
Cybercrime (procedural)	*Established*	Computer Crimes Act 2003 provides for preservation of data, search and seizure (including without warrants) and interception of electronic communications. Mutual Assistance in Criminal Matters Act and the Extradition Act allow for international cooperation between countries involved in the prosecution of offences.
Law enforcement	*Initial*	Law enforcement capacity is low. Tonga Police primarily utilises AFP and New Zealand Police resources to investigate cybercrime, although the transnational crimes unit is building capacity and is looking to reconnect with INTERPOL, primarily for cybercrime

		matters. Tonga is a member of the Pacific Transnational Crime Network. Tonga relies on the CERT for forensic and other investigation support. There is no clear enforcement strategy or enforcement protocol across stakeholders.
Prosecution	*Initial*	Prosecution capacity is low. A concern was expressed to us that the current Computer Crimes Act doesn't contain relevant offences for successful prosecution.
Courts	*Initial*	Low judicial capacity, although as part of Budapest Convention process, the DPP, lawyers and judges are given access to Council of Europe training to assist in capacity building for prosecuting and hearing cybercrimes.

Safeguarding electronic transactions

Legal and regulatory frameworks		
Electronic transactions	*None*	A draft Electronic Transactions Bill, drawing upon the UNCITRAL Model Law on Electronic Commerce and Model Law on Electronic Signatures, was prepared in 2014. Progress on this bill has stalled pending the implementation of the new Computer Crimes Bill. E-government was a priority for a previous Minister, but is not currently a priority and officials are unsure of how quickly legislation and regulatory frameworks supporting electronic transactions and e-government will be developed and implemented. Tonga has recently requested that a "Rapid e-Trade Readiness Assessment" be conducted by UNCTAD.
Privacy, freedom of speech and other human rights online	*None*	No general protections identified. Not a priority area, although social awareness programmes around cybersecurity and associated rights, like privacy, are running primarily through community outreach programmes sponsored by MEIDECC.
Data protection	*Initial*	A draft Privacy Bill, drawing upon the Australian Privacy Act (Cth) and the New Zealand Privacy Act, was prepared in 2014. We understand this work is at an early phase, and has not been progressed for some time. E-government was a high priority some years ago, but is not currently a high priority and officials are unsure of how quickly legislation and regulatory frameworks supporting electronic transactions and e-government will be developed and implemented. We note that in our view, the draft Privacy Bill is not fit for purpose for a country the size of Tonga. Some specific legislative provisions restrict use of information by government. In particular, the Official Secrets Act criminalises the communication or retention of any information by a government employee without authorisation. The Statistics Act 2015 also limits use of information obtained under that Act to statistical purposes, and the Criminal Offences Act contains certain offences relating to the misuse of information, including fraud, forgery and procuring the execution of documents on false pretences.
Digital authentication	*Established*	National identity card system, administered under the National Identity Card Act 2010. We understand the identity cards are now

Legal and regulatory frameworks		
		commonly used for general identification purposes, as well as voting in national elections.
ccTLD administration	*Initial*	Tonga's ccTLD is .to, and is administered by the Tonga Network Information Centre.
Consumer protection	*Established*	There is a Consumer Protection Act 2000, but it does not contain any specific provisions concerning online activity. A Consumer Protection Bill has been developed, but is yet to be finalised.
Intellectual property legislation	*Established*	Tonga has a Copyright Act 2002, as well as other intellectual property legislation, but no provisions specifically address online intellectual property.
Access to information	*Initial*	Tonga has a freedom of information policy, developed in 2012 by a Cabinet steering committee. However, Tonga also has an Official Secrets Act, under which it is an offence for any Tongan official to disclose information obtained in his/her office, where this disclosure is contrary to his/her official duty or otherwise not in the public interest. There is consequently some potential for conflict with the freedom of information policy.

Recommendations

On the basis of our desktop review and consultation mission to Tonga, our recommendations are as follows:

- *Cybersecurity strategy*: We understand that developing a cybersecurity strategy is on MEIDECC's agenda once the Computer Crimes Bill is enacted. We encourage MEIDECC to bring the CERT stakeholders into the taskforce to develop Tonga's cybersecurity strategy and to coordinate with other Pacific countries in developing that strategic framework.
- *Cybercrime investigation and enforcement framework*: Tonga's new Computer Crimes Bill is likely to provide a strong legal framework for cybersecurity issues, but without investigation and enforcement capability, the law will not be effective. In order to improve investigation and enforcement capability, there should be a focus on capacity building for investigators, prosecutors, law practitioners and the judiciary.
- Further, in order to ensure effective coordination between key stakeholders, we recommend that stakeholders enter into memoranda of understanding and/or enforcement protocols which clearly set out which agencies are responsible for aspects of investigating and enforcing cybercrime (including the role of ISPs and CERT) and processes to be followed in response to an incident.
- We also recommend that to ensure the effectiveness and long-term sustainability of Tonga's CERT, it should be adequately funded and resourced. We understand that the CERT is being called upon to provide forensics and other skills, but is not currently funded (and therefore lacks the resources) to do that work, as well as build capacity and function as a response team for cyber issues.
- *CERT Capacity building:* The CERT currently has only 3 dedicated employees. The CERT could become a hub for knowledge, incident response as well as providing input into policy and budget for cyber and digital issues generally, in the absence of a specific cyber/digital focal point in Government. In order to do that, it will need more resources, and will need to work closely with other CERTs to develop best practice guidelines.
- *Digital economy frameworks*: MEIDECC and the Attorney General's office have confirmed that there are plans in place to develop electronic transactions legislation and e-government initiatives following the

enactment of the Computer Crimes Bill (as above, a draft Electronic Transactions Bill was developed in 2014, but not progressed). We recommend that in order to effectively develop these initiatives, MEIDECC and the Attorney General's office are funded to look at other jurisdictions where these initiatives have been implemented well and map this against Tonga's economy, social structure and size. We also recommend awareness building in the community to coincide with the development of the legislative and regulatory framework. We understand from our in-country visits that currently social awareness is relatively low in terms of individual's online rights and online safety. While Tonga Police run a social awareness programme around cybersecurity (and, in particular, child protection and exploitation), general digital awareness is relatively low.

Tuvalu

Summary

Tuvalu does not have a national cybersecurity strategy or specific laws relating to cybersecurity. A draft Cybercrime Bill is in the development process, and is expected to be ready for enactment in 2019. Tuvalu does have some general offence provisions and search and seizure rules that may be applied to online activity.

The Ministry of Communications, Transport and Tourism is responsible for ICT matters, including cybersecurity. Tuvalu's police force also has some involvement with cybersecurity issues.

The Tuvalu legislative framework for safeguarding electronic transactions, and related areas, including data protection and consumer protection, is relatively undeveloped. We understand this lack of development reflects the limited use of electronic transactions in Tuvalu at present.

To give a sense of scale, an estimate of the size of the population in Tuvalu is 11,300 people.

Cybersecurity

Strategy and governance		
National cybersecurity strategy	*Initial*	Tuvalu's National Strategy for Sustainable Development 2016-2020 includes a number of strategies and targets relating to ICT development and refers to the intended development of cybercrime legislation. We understand that some consideration was given during the early 2000s to developing a National ICT Policy, although the process has since stalled.
Governance	*Established*	The Ministry of Communications, Transport and Tourism has general responsibility for ICT matters and is Tuvalu's contact point for cybersecurity issues. The Attorney General's Office has responsibility for prosecution and Tuvalu police force has responsibility for law enforcement.
Security		
Institutions	*Initial*	As above, the Ministry of Communications, Transport and Tourism has general responsibility for ICT matters, including cybersecurity. Tuvalu does not have a CERT.
Critical infrastructure	*None*	No cybersecurity arrangements for critical infrastructure identified.
Vigilance		
Incident reporting	*Initial*	Cybersecurity incidents can be reported to the designated officers in the police force or the Director of the ICT Department. No mandatory reporting requirements have been identified. Tuvalu does not have any general cyber awareness-raising programmes underway. Raising awareness of cyber risk is a priority for the Ministry of Communications, Transport and Tourism.

Domestic cooperation	*None*	No formal domestic cooperation arrangements identified.
International cooperation	*Initial*	Tuvalu is a member of APT, CTO, PaCSON, PICISOC, PICP, PITA and PTCN. Tuvalu is a participating country for the PIRRC and is among the beneficiaries of the ICB4PAC project. Tuvalu is involved in Cyber Safety Pasifika. Tuvalu has some international law enforcement links, including to the AFP (with the Pacific Police Development Program) and the New Zealand Police (with the Pacific Island Prevention Programme). The Extradition Act and Mutual Assistance in Criminal Matters Act would apply to cybercrime, if criminalised, in Tuvalu.
Resilience		
Cybercrime (substantive)	*Initial*	A draft Cybercrime Bill has been prepared and was reviewed in March / April 2018 against the Budapest Convention standard. This review led to some recommendations for improvements, which the Attorney-General's Office is considering. Consultations will be undertaken before the Bill is submitted for enactment (likely to be 2019). The Tuvalu Telecommunications Corporation Act includes some offences, including for interference with messages, interception and disclosure of intercepted messages, and sending grossly offensive messages. The Penal Code sets out non-specific fraud and forgery offences.
Cybercrime (child protection)	*None*	Tuvalu has acceded to the Convention on the Rights of the Child. Tuvalu has developed a draft Child Protection and Welfare Bill, to address its obligations under the Convention on the Rights of the Child. No other child protection legislation identified.
Cybercrime (procedural)	*Initial*	The Criminal Procedure Code(s 101) and the Police Powers and Duties Act (s 61) contain general powers of search and seizure, which may apply to electronic evidence.
Law enforcement	*Initial*	The Tuvalu National Police is responsible for investigating crime. Two officers have been designated to handle such cases. Capacity of the police force to handle cybercrime appears to be low.
Prosecution	*Initial*	We expect prosecution capacity to be low, given the limited cybercrime training for the police and the lack of cybercrime prosecutions.
Courts	*Initial*	We expect judicial capacity to be low, given the limited cybercrime training for the police and the lack of cybercrime prosecutions.

Safeguarding electronic transactions

Legal and regulatory frameworks		
Electronic transactions	*None*	No electronic transactions legislation identified. Use of electronic transactions in Tuvalu is limited (for example, there is no local electronic banking or credit card usage). Tuvalu has recently requested that a "Rapid e-Trade Readiness Assessment" be conducted by UNCTAD.
Privacy, freedom of speech and other human rights online	*Initial*	The Tuvalu Constitution sets out fundamental rights to freedom of expression and to privacy of the home and property. In 2014, Tuvalu appointed an Ombudsman, although the focus of the role appears to be on reducing corrupt practices in government.
Data protection	*None*	No general data protection legislation identified.
Digital authentication	*None*	No digital identification scheme identified.
ccTLD administration	*Established*	The .tv domain is an open ccTLD and is managed by the Ministry of Finance and Tourism. The registry is operated under contract by .tv Corporation International, a for-profit Verisign company. The Uniform Domain Name Dispute Resolution Policy applies.
Consumer protection	*None*	No consumer protection legislation identified.
Intellectual property legislation	*Initial*	Tuvalu has a Copyright Act 2008, which criminalises copyright infringement. Tuvalu has also enacted a Registration of UK Patents Act, a Registration of UK Trade Marks Act and a UK Designs Protection Act, which provide protection for certain intellectual property rights recognised in the United Kingdom.
Access to information	*Initial*	The Tuvalu Constitution recognises the right to freedom of information. No general access to information legislation identified.

Recommendations

On the basis of our desktop review and discussions with Tuvalu representatives, our recommendations are as follows:

- *Develop cybersecurity strategy*: Tuvalu should consider developing a cybersecurity strategy document, which outlines the country's risk profile, and a plan to strengthen Tuvalu's cyber framework. It could also clarify roles and responsibilities (within the public and private sectors) for managing cyber risk. One option might be to include this strategy in the next iteration of Tuvalu's National Strategy for Sustainable Development, which will presumably run from 2020 (when the current strategy ends).
- *Strengthen cybercrime framework*: Under its existing legal framework, Tuvalu would not be able to prosecute most cybercrime activities. Tuvalu should continue to develop specific cybercrime legislation, drawing on the Budapest Convention and reflecting Tuvalu's specific circumstances. In tandem, Tuvalu should also ensure that its criminal procedure law is relevant and appropriate to cybercrime cases, including confirming that electronic records are admissible, and setting criteria for the integrity of electronic records.

Additional resourcing and training may also be required to ensure that law enforcement, prosecutors and the judiciary are well-equipped to deal with cybercrime cases.

Vanuatu

Summary

Vanuatu has an established National Cybersecurity Policy in place and has a designated agency responsible for cybersecurity, the Office of the Government Chief Information Officer. As part of the implementation of the National Cybersecurity Policy, Vanuatu has recently established a CERT, to implement cybersecurity policy and coordinate incident response across public and private sectors.

Some general legislation can be applied to cybercrime activities. A Cybercrime Bill, drawing on the Budapest Convention, is in the process of being developed.

Vanuatu also has a relatively well-advanced legislative framework for safeguarding electronic transactions and resolving digital legal issues.

To give a sense of scale, an estimate of the size of the population in Vanuatu is 282,100 people.

Cybersecurity

Strategy and governance		
National cybersecurity strategy	*Established*	A National Cybersecurity Policy was finalised in December 2013, and sets out Vanuatu's plans to develop an organisational structure for cybersecurity, operational standards for critical infrastructure, a stronger legal framework, improved capacity for stakeholders and better international cooperation frameworks. We understand this policy is in the process of implementation.
Governance	*Established*	The Office of the Government Chief Information Officer is responsible for cybersecurity policy. The Office of the Telecommunications and Radio-communications Regulator is responsible for regulating the ICT sector generally. Other relevant stakeholders include the Ministry of Justice (leading child protection work), the Public Prosecutor, the Vanuatu Police and the Chamber of Commerce.
Security		
Institutions	*Sophisticated*	As noted above, the Office of the Government Chief Information Officer has primary responsibility for cybersecurity policy. Vanuatu's National Cybersecurity Policy also notes an intention to establish: • a National Cybersecurity Steering Committee responsible for ICT and implementing the Cybersecurity policy; • a child online protection working group to identify areas for child online protection; and • a unit within law enforcement that serves as single point of contact for requests from government institutions as well as citizens and businesses. In June 2018, Vanuatu launched a CERT, with support from the Australian Government and APNIC.

Critical infrastructure	*Initial*	No cybersecurity arrangements for critical infrastructure identified, although the National Cybersecurity Policy notes the intention to identify the operators of critical infrastructure and develop minimum technical standards to be applied by these operators.
Vigilance		
Incident reporting	*Initial*	Incidents can be reported to the Crime Prevention Unit of the Vanuatu Police Force. No mandatory reporting obligations have been identified. Vanuatu is a participant in Cyber Safety Pasifika, and has also undertaken some ad hoc awareness-raising campaigns.
Domestic cooperation	*Initial*	Procedures for standardisation of ICT hardware and software use by government agencies are set out in the Council of Ministers Decision 06: Information Systems, Infrastructure and Service Management Strategy, including the establishment of a cross-ministry committee. No other formal domestic cooperation arrangements identified, although the National Cybersecurity Steering Committee envisaged by the National Cybersecurity Policy would presumably be instrumental in this regard.
International cooperation	*Established*	Vanuatu is a member of APT, CTO, ITU-IMPACT initiative, PaCSON, PICISOC, PICP, PITA, PTCN and Interpol. Vanuatu is a participating country for the PIRRC and is among the beneficiaries of the ICB4PAC project. There is an Interpol office in Vanuatu. Vanuatu's Office of the Public Prosecutor seeks to improve its links with counterparts in Australia and New Zealand, so that assistance with cybercrime matters is available when needed. Vanuatu's Police has some links with the AFP (including access to AFP advisors under a direct cooperation programme) and to the New Zealand Police (with the Pacific Island Prevention Programme). Mutual legal assistance and extradition legislation is in place, with the Mutual Assistance in Criminal Matters Act 2002 and the Extradition Act 2002.
Resilience		
Cybercrime (substantive)	*Initial*	The Telecommunications Act criminalises intentional damage of a telecommunications system, wilful interception of a telecommunications transmission, and interception and disclosure of telecommunication messages. The Penal code also criminalises the disruption of a computer system or essential services, where the disruption occurs as part of a terrorist act, and includes general offences for fraud and forgery. Vanuatu prepared a Cybercrime Bill in 2015, drawing upon the Budapest Convention, with substantive criminal law provisions to enable prosecution of cybercrimes including illegal access, data interference, computer related fraud and cyber stalking. The Bill is currently in a process of revision, with assistance from the Australian Attorney-General's Department. If completed in time, the Bill will be tabled in Parliament at the end of 2019. We understand a draft Spam Bill is also under development.

Cybercrime (child protection)	*Established*	The Penal Code includes offences for possessing, publishing and creating child abuse material, obscene publications and indecent exposure, although these offences do not explicitly address online activity. The Cybercrime Bill includes further offences relating to child abuse material. Vanuatu has signed and ratified the Convention on the Rights of the Child and the Optional Protocol on the Sale of Children, Child Prostitution and Child Pornography.
Cybercrime (procedural)	*Initial*	The Criminal Procedure Code includes powers for search and seizure that extend to electronic evidence. The Cybercrime Bill includes procedural powers for the search and seizure of stored computer data (including production orders), real-time collection of computer data and other powers necessary to investigate cybercrimes.
Law enforcement	*Initial*	The Crime Prevention Unit of the Vanuatu Police Force is responsible for cybercrime cases. We understand the Police Force is limited when dealing with cybercrime cases by a lack of computer training and computer literacy. Building capacity for cybercrime investigations is a key focus going forward. Registration of SIM cards is not required, making it difficult for the Police to identify the senders of some electronic communications. Mandatory registration is currently being considered by the Office of the Telecommunications and Radio-communications Regulator.
Prosecution	*Initial*	We expect prosecution capacity to be low, given the limited cybercrime training for the police and the lack of cybercrime prosecutions.
Courts	*Initial*	We expect judicial capacity to be low, given the limited cybercrime training for the police and the lack of cybercrime prosecutions.

Safeguarding electronic transactions

Legal and regulatory frameworks		
Electronic transactions	*Established*	The Electronic Transactions Act 2000 makes provision for electronic records, communication of electronic records, electronic signatures, encryption and data protection, and intermediaries and e-commerce service providers. We understand there is some concern in Vanuatu that this legislation may now be outdated. Other relevant legislation provisions include: • The Personal Property Securities Act 2008: ss 159 and 163 allow notice to be served by electronic mail; writing includes the recording of words by electronic means; s 19 security agreements can be electronic. • E-Business Act 2000: Part 2 deals with Cybersuite contracts and electronic business contracts; Part 3 deals with e-business accounts.

Legal and regulatory frameworks		
		• Companies Act 2006: s 396 provides for companies to keep records electronically. UNCTAD completed a "Rapid e-Trade Readiness Assessment" for Vanuatu in 2018.
Privacy, freedom of speech and other human rights online	*Initial*	The Constitution of Vanuatu recognises freedom of expression and privacy of the home and other property as fundamental rights.
Data protection	*Initial*	The Telecommunications and Radiocommunications Consumer Protection Regulation restricts the use of consumer information by telecommunications service providers. No general privacy or data protection legislation identified.
Digital authentication	*None*	Vanuatu has a national identity card scheme, primarily for use when voting in elections. No link between this scheme and digital authentication identified.
ccTLD administration	*Initial*	The .vu domain name is managed Telecom Vanuatu Ltd, although the Office of the Telecommunications and Radio-communications Regulator has conducted a public consultation on the future management of this ccTLD. No dispute resolution procedures identified.
Consumer protection	*Initial*	The Telecommunications and Radiocommunications Consumer Protection Regulation provides various regulatory protections to consumers of telecommunications services.
Intellectual property legislation	*Established*	Vanuatu has a Copyright and Related Rights Act 2000, which includes an offence for international and for-profit infringement of copyright. Vanuatu also has enacted the Patents Act 2003, Registration of United Kingdom Patents Act, Registration of United Kingdom Trade Marks Act and Trademarks Act 2003.
Access to information	*Established*	Vanuatu has enacted the Right to Information Act 2016, which provides for the exercise of a right to access information held by both public and (in some circumstances) private agencies.

Recommendations

On the basis of our desktop review and discussions with Vanuatu representatives, our recommendations are as follows:

- *Implementing the National Cybersecurity Policy*: Vanuatu has a well-drafted cybersecurity strategy in place, and has made significant progress in implementing this strategy, including with the creation of a CERT. The next step is to continue implementing this strategy, including the cooperation frameworks (domestic and international) and management of critical infrastructure.
- *Continue development of the Cybercrime Bill*: The enactment process for the Cybercrime Bill should continue.
- *Increase enforcement capacity:* At the same time, it will be important to focus on the resources and training available to law enforcement, prosecutors and the judiciary in dealing with cybercrime cases, so that the legislation can be enforced once enacted. Capacity building may include establishing a cybercrime unit within the police and improving coordination of cyber stakeholders. Another recommendation noted by stakeholders is strengthening external assistance with other countries as the current Mutual Criminal Assistance processes are too slow.
- *Privacy and data protection framework*: The Telecommunications and Radiocommunications Consumer Protection Framework is a useful starting point for protecting the personal information of consumers. While cybersecurity is a priority, when reform capacity allows we suggest Vanuatu consider enacting a general privacy and data protection framework, as and when needed to manage risks arising from the uptake of digital technologies in Vanuatu and to support Vanuatu's move to a digital economy.


PRIF


ADB


Australian
Aid


European Union


JICA


NEW ZEALAND
Aid Programme


WORLD BANK GROUP