

e-talanoa

WEBINAR

CYBER SAFETY DURING AND POST COVID 19 CRISIS

Pacific Islands Chapter

www.picisoc.org Internet Society

THURSDAY 29TH OCTOBER 2020

07:00 PM Fiji Islands, Marshall Islands

E-Talanoa Webinar on Cyber Security During and Post COVID19 Crisis

Thursday 29 October, 2020



@PICISOC #eTALANOA

William Tibben, University of Wollongong

Internet Society Pacific Islands Chapter

William Tibben

Good evening, everyone, and thank you very much for your participation, your attendance at the second E-Talanoa, staged on behalf of the PICISOC Board, and on their behalf I'd like to welcome everyone there, everyone here. My name is Will Tibben, I'm at the University of Wollongong, and

I've been a PICISOC member since about 2006. I spent some time on the board around 2012, and I have remained a member. My job, really, today is just to make way for other people to speak.

So, I'm not going to take too much of your time, just to maybe recap, or kind of explain, the E-Talanoa concept, which is essentially a Polynesian term or word which relates to storytelling. Its features really relate to respectful tolerance, and also just listening to what other people have to say about topics of concern, and it's through this kind of dialogue, where everyone gets to talk, and not only talk, but also listen, that we can come to new understandings about complex problems.

Today's topic on cybersecurity is one that is looking at cybersecurity in this particular time of COVID and beyond, and that's what today's speakers are going to be speaking about. And also the specifics as they relates to the Pacific cybersecurity policy, its applications, in some sense this is in its early stages of development, and certainly a lot of work's been done. And things have, as you could say, transforming with digital transformation, we're getting to learn more about cybersecurity policy and the like.

Without further ado, I will introduce you to tonight's speakers. We've got Anne Dunn-Baleilevuka, Anne's is the Commissioner for Online Safety in Fiji, so thank you very much, Anne, for making your time available and speaking. We have Torrin Marquardt from Standards Australia. Torrin's current role is International Engagement Manager for Standards Australia. We have Suetena Faatuuala Loia from the Ministry of ICT, from Samoa. Suetena is the Acting Chief Executive Officer for Information Communication Technology. We have Klee Aiken from CERT New Zealand, Klee's the Principal Pacific Partnership Advisor. So, welcome, Klee. And we have Kensly Joses from CERT in Vanuatu, and Kensly's currently the Officer in Charge.

Each of the speakers will talk for about 10 minutes, and I encourage you, if you've got any questions while we're talking, while the speakers are doing their presentations, please put them in the chat and we will attempt to get to the questions, probably after everyone had their talk, had spoken, and we'll open it up for discussion. If you've got specific questions to specific people, just make that clear in the chat.

Without further ado, I will pass you over to Anne, thank you very much Anne. If you'd like to start. If you've got slides to share, there's generally a share button down the bottom of the screen which you can, if you click on that, you'll be able to share your screen, but there's no obligation to have slides or anything like that.

And sorry, I actually forgot to introduce Cherie, who's the Chairman of the Board, Cherie Lagakali, and Tim, Timoci Tuisawau from the PICISOC Board, thanks for making this possible. So, Anne, I'll hand it over to you. Thank you.



Anne Dunn-Baleilevuka

Thank you. Just let me know if you can't hear me, but bula vinaka, and good evening.

Thank you so much for just the opportunity to sort of share on this topic. I'm really just coming at this more from a broad perspective of cybersecurity, I guess, in Fiji, but more particular to online safety, and then more specifically to the Online Safety Commission's experience with COVID-19. And then what we're seeing, as we transition into the post COVID-19 world, or post-pandemic world. And so, I'd be really interested in any questions that you may have, throughout the presentation. I don't at this stage have any slides to share, so it's really just me talking for the next 5 to 10 minutes. I'm going to try to keep it as short and simple as possible.

A brief bit of background on the Commission itself. It's a recently established Commission that was set up by the Online Safety Act here in Fiji. We had started operations from last year, and so we've been running for about 22 months now. The COVID-19 pandemic really brought out the grave need for infrastructure, and more of a collective approach, towards online safety and cybersecurity as a whole.

We're seeing that, during the COVID-19 period here in the country, when the virus had initially been introduced to our shores, there was a lot that took place online. A lot of information was shared online about the virus. A lot of information was shared in an effort to get information out there, because it was the most prominent way to really exercise, and deal with, what was

happening globally. It was a good platform to get information out as quickly as possible so that individuals could safeguard themselves. In that the Commission took the role of really just maneuvering with the information that was being put out.

As the Commission, we act primarily to promote online safety in the country and raise community awareness, particularly around digital literacy, and really working with communities. We work strongly with Fiji Police in terms of raising awareness in the country. That was one of the most effective ways that we were able to engage with communities last year. We were also able to go out to schools, gauge what schools understood of online safety in general.

The Commission itself is also able to receive complaints of online abuse. That's particular to online abuse in the sense of online bullying, or image-based abuse, or something that's affecting the individual. It's not necessarily hacking, or cybersecurity threats, or cyber threats, that are affecting the infrastructure, or the computers, and its networks. It's more to do with the individuals, which is why this conversation from my end will be most likely for the individual itself, and the experience that people have online.

During the COVID-19 period, we had noticed this really big shift of information that was being shared online, and how that was being shaped for us here in the country. We had information that was going out online in an effort, for health reasons, obviously, to be able to protect people. But what we could have done better, for us, was that we could have understood the dynamics of what information was to be shared, as early as possible, which we had learned in the first couple of weeks when the virus came. It developed then into April, and May, and June, when information started going out.

And it was more broad in the sense that details of individuals were no longer being shared, which was really good. In the beginning it seemed like anything and everything to protect individuals, was being shared online. That was something that we really noticed throughout the COVID-19 period. The Commission received a lot of reports of, mostly, comments relating to personal information that was being shared. We received reports regarding online abuse that was in the realm of image-based abuse, that went up from the amount of reports that we received last year during the same time. We also received reports that were around defamatory comments, which weren't necessarily something that had to do with the virus itself or the pandemic. Then further to that, we noticed -- there weren't any reports lodged specifically with the Commission, but we noticed -- a trend of information that was being shared with regards to the remedies to the virus. That was big here in the country, because we're very communal, but we're also very sensitive to

how we use natural medicine. A lot of that took a role in the type of information that was being shared online.

In terms of cybersecurity, as a whole, the threats were definitely there, but government initiatives definitely took the steps to keep individuals guarded. There were different technologies that were used to contain the spread of the virus, there was a new Care Fiji App that was launched, during the COVID-19 experience here, to help contain the virus, different health messages went out on, particularly, social media platforms, and then, subsequently, to traditional media.

But, in a post COVID world, one thing that we are seeing a transition in how different technologies are used in the country, because education was really one of the biggest things that took a toll, in the sense that we didn't have the infrastructure set up for education to be done so widely, so rapidly. Although we have the networks available, and people have access to the Internet, it was securing those Internet platforms, that is definitely a lesson, and a takeaway, that we bring from this.

With regards to the national cybersecurity policy, there was one that was initiated earlier in, I want to say, 2013. There's a national policy that's currently in place. There is also cybercrime bill that's in the country, and that's specific to cyber crimes, but it's still being tabled in Parliament. I'm sure that the national security, national cybersecurity policy is also up for review, but we currently have one, and I know that it's also being worked on for review. Just in terms of that question from Rajnesh, yes, it was already developed. I think it's just being fine-tuned, although it has a lot of room to grow, because of how technologies have changed from the time that it was put together.

I think at this point, that's where I'm going to leave this part of my talk, but if there's definitely any questions, I am looking forward to answering them. I see one from Elaine, and if I can answer them now?

A few of the challenges, that we have faced from establishment, is really just integrating law enforcement and the commission. We did that through the MOU that was signed with Fiji Police and OSC earlier this year, and so we were able to integrate that. The Commission is an independent body in its legal form. We are a corporate body that's able to represent ourselves. However, with the Information Act, we're legally bound by the definition of being a government agency. So, there's a bit of a tricky relay on that second question. It's independent in the sense that we are a corporate body able to act as our own but, in light of the Information Act, we're also representatives of government agencies, as defined by that act.

The cybercrime bill is specific to cybercrime in the country, and it's not necessarily relative to the different sectors of the economy. I'm not sure if I'm answering that question correctly, but if the question is for the cybercrime bill that's currently in Parliament, the cybercrime bill is only specific to aligning Fiji to the Budapest Convention, which is the only international binding convention that holds us for anything related to cyberspace. And so, the cybercrime bill is detailed for that interlining, or integration, of the Budapest Convention, so that we can become a party to that convention.

William Tibben

Thank you very much, Anne, that was great. I'm sure we'll get some time later on to follow on with some of these questions.

Now, I'll introduce Torrin Marquardt from Standards Australia. Standards Australia have been doing work in the Pacific, informing people about the ISO 27000 standards. Torrin is gonna speak a bit more about that. Thanks, Torrin.

Torrin Marquardt

Thank you. Well, I'm just going to share my slides. Give me one moment here.



@PICISOC #eTALANOA *Torrin Marquardt, Standards Australia* Internet Society Pacific Islands Chapter

Thank you to PICISOC for the invitation to speak this evening. My name is Torrin Marquardt and I'm an International Engagement Manager at Standards Australia, and I'm here to talk to you a bit about cybersecurity standards.



First, I'll give you a bit of background about Standards Australia. We're an independent, not-for-profit organization, and this is not typical as a national standards body. Many national standards bodies around the world are actually part of government, including those standards bodies in the Pacific region. But we are recognized by the government as the peak National Standards body in Australia, and we represent Australia and Australian interests at two of the world's biggest international standards bodies. So those are the International Organization for Standardization, or ISO, and the IEC, which is the International Electrotechnical Commission. We are a member-based organization and our work schedule and agenda is driven by Australian stakeholders, and serving the Australian community.



What is a standard?

Standards are a voluntary, consensus solutions

They document an agreement on how a material, product, process, or service should be specified, performed or delivered

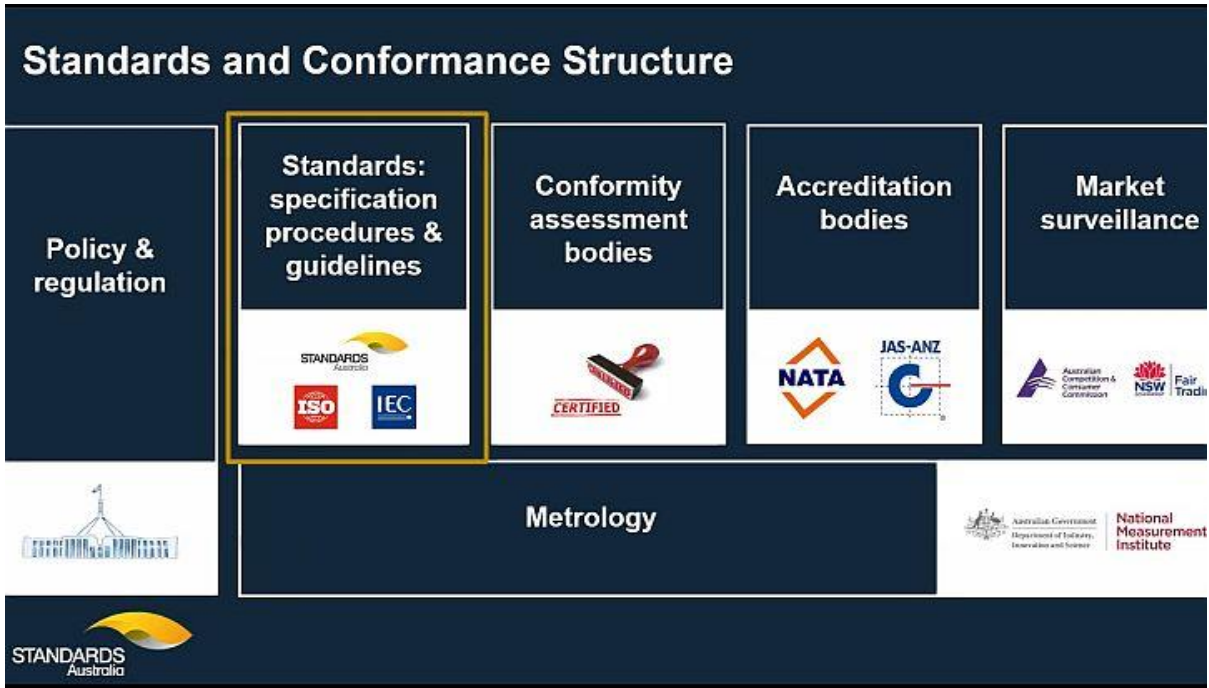
They provide a common and repeatable basis for doing things and help bring 'order' to the world

The first question some of you might have is what is a standard? If you come from a technical background you might be very familiar with them, but many people are not familiar with them. I'll just give you a brief overview. Essentially, a standard is a document that sets guidelines for how a product or service should be designed, and how it should perform, and they are developed through a consensus-based process. We bring together a broad range of experts, technical experts, to agree on best practice and on the content of the document. There are international standards, there are national standards, and in the case of cybersecurity, we'll be speaking about international standards.

In bringing together the experts to create these documents, that could include experts from -- if you're looking at cybersecurity, it could include ICT providers and manufacturers, government and public agencies, academia, businesses, consumers -- a whole range of experts. Really to ensure the integrity of the document, and follow this consensus-based process, you want to have as broad a range of interests involved as possible. In other words, the standard is an industry-backed document to a market-based problem.



An important thing to note is that our standards are voluntary documents. However, they can be referenced in legislation, and this then makes them mandatory. Just as an example, there are many Australian standards for building and construction that are referenced in our building code, which then makes them mandatory. So, for the topic of today's webinar, standards for cybersecurity could also be used to support national cyber policies.



One quick thing to note is that standards are just one part of quality infrastructure. This framework also includes certification, accreditation, testing, metrology. All of these elements sit alongside policy and regulation. Standards Australia is responsible solely for standards development activities. However, some standards bodies in the Pacific actually look after all of these different pillars of quality infrastructure.



As I mentioned at the beginning, we're the representative at those two major standards organizations, ISO and IEC, and they are responsible for developing international standards, across a range of sectors, including ICT and cybersecurity standards. We're also a member of the Pacific Area Standards Congress, or PASC, which is a regional body which focuses on collaboration in the standard space. We're seeing standards bodies grow in importance around the world, and really in the Pacific region as well. We engage quite a bit with the region and, at the moment, Fiji, PNG, and Vanuatu are members of ISO. We're seeing a few other countries, as well, taking steps to become members. I would anticipate that this trend will continue to grow, and we hope to continue working with the region on this. An important thing to note, too, is having a standards body serves as your country's gateway into these international bodies, your gateway to the adoption of international standards, and the use of international standards.



Cyber Security in a COVID-19 World

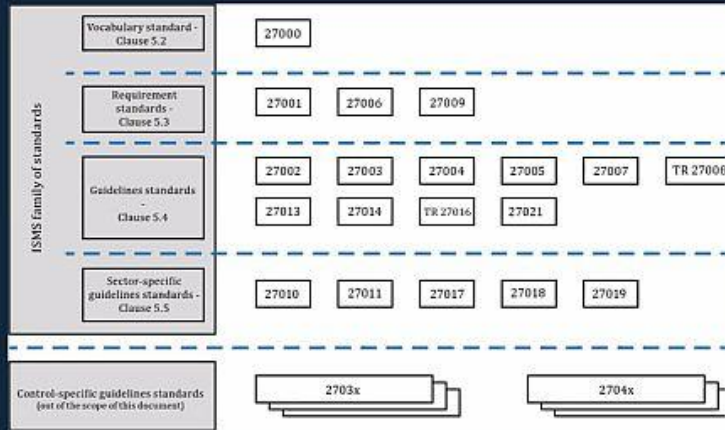
- Rise in phishing and ransomware attacks
- Increased security risk in working from home (dependence on VPNs)
- Potential delays in detection and response to cyber attacks
- Exposed physical security (working from cafes, etc.)
- Increase in cyber criminals (with economic effects of COVID-19)

Source: Deloitte 2020

Now that I've given you a bit of background, which I hope was useful, we can switch over to the specific topic of cybersecurity, and looking at cybersecurity in a COVID-19 world. The pandemic, without a doubt, has pushed us all to embrace new ways of working, new ways of communicating. Tonight's session is a perfect example of that. Although it has brought some greater efficiencies and flexibilities in how we work, it also has introduced an increase in cyberthreats. For example, for those working outside of the office, there's more work to be done by your IT teams to make sure that your networks are kept safe. From a physical security perspective, too, there's an increased risk, if you're taking your laptop home with you, and traveling with it, the possibility of leaving it somewhere, or having somebody steal it, that risk is increased. Also, with economies around the world hit hard by the pandemic, there's been an increase in cybercrime activities and cyberattacks. The point that I want to make here is that having standards and systems in place, to keep your information safe, has therefore never been more important than it is today.

What is the ISO/IEC 27000 Series?

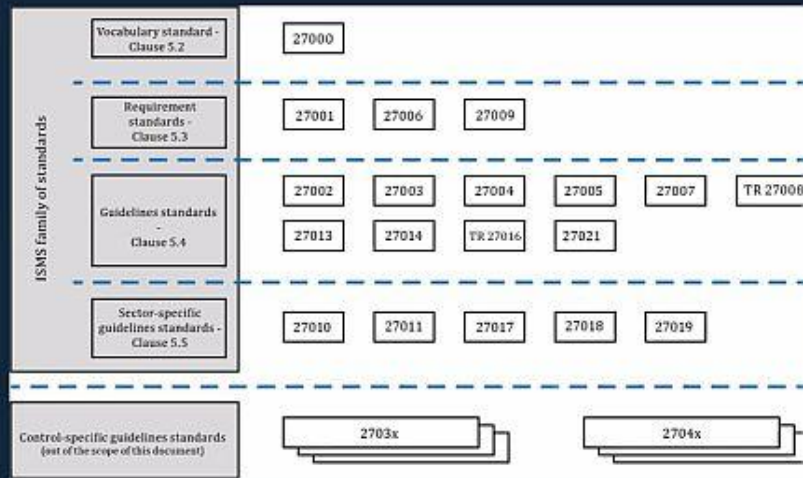
- The ISO/IEC 27000 family of standards helps keep information secure.
- There are around 45 standards in the 27000 family.
- ISO/IEC 27001 is the best-known standard, providing requirements for an information security management system (ISMS).



Now to look specifically at one particular series of standards that were mentioned in the introduction. It's a bit of a mouthful, it's called the ISO/IEC 27000 Series. It's a family of standards providing best practice recommendations on all things Information Security Management. It helps protect the security of assets, and this can include financial information, intellectual property, employee details, all sorts of private data like that. There are about 45 standards in this series but 27001 is kind of the foundational standard, the most well-known one, the one that people tend to start with, and it provides requirements for an Information Security Management System, which is a systematic approach to managing sensitive company information. It's essentially a framework that considers an organization's people, processes, IT systems, and then applies a risk management process across the board. It's designed to help organizations of all sizes, of all sectors, from SMEs through to your larger ones, and is one of the most used international standards in the world, and a key part of the suite of standards on cybersecurity.

What is the ISO/IEC 27000 Series?

- The ISO/IEC 27000 family of standards helps keep information secure.
- There are around 45 standards in the 27000 family.
- ISO/IEC 27001 is the best-known standard, providing requirements for an information security management system (ISMS).



Although the series is intended for use by organizations and businesses, I also just wanted to highlight that the standards also play a big role for consumers and the community more broadly.

As an employee at work, for example, you put trust in your organization that your personal information is going to be safe and secure. This could be anything from your home address, or bank information, or even work-related data through your email inbox. We put this trust every day in our organization that that information is going to be kept safe. But how do we know that it will be kept safe? If your organization has standards in place, it gives you that greater confidence that there is a safeguard, that there is a system in place that's following international best practice, that's been agreed upon by experts all around the world. The same can be said for products or services that you might be using, for example, if you're making purchases online, or accessing other digital platforms, having that assurance that the businesses that you're engaging with are adhering to standards as well. In short, cybersecurity standards build trust for consumers and businesses alike, when it comes to sharing private data and using digital services and platforms.

More than just cyber safety...

1. Interoperable solutions.
2. Proven and efficient methodologies.
3. Worldwide access to expertise.
4. Tools and techniques easily accessible.
5. Established certification infrastructure.
6. Supports trade.
7. Provides the ability to demonstrate capability.

Cost and
Time Savings
+
Effective
Solutions
=
Sustainable
Cyber Security
in your Country



Another point just to add. I won't go through this full list, but cybersecurity standards do a lot more to than just addressing cyber safety. They provide interoperability between different systems so that they can talk to one another and provide a tried and tested solution rather than starting from scratch. By using an international standard, if it's the same standard that countries around you are using as well, it opens up opportunities for trade. Also, as the world changes, and particularly in the cyberspace where things seem to be changing incredibly rapidly, standards are regularly updated as well to address these changes and support innovation, and address any new challenges that might arise.

Cyber Security Regional Standardisation Enhancement Program



Fiji



Papua New Guinea



Solomon Islands



Tonga



Vanuatu



Lastly, I'd like to briefly talk about a piece of work that we did in the region last year. I think I actually saw [Siosaia Vaipuna] on the line as well, who was involved in the work. So hello, Saia. The work that we did was related to the ISO/IEC 27000 series. We partnered with the five countries you can see on the screen here, Fiji, Papua New Guinea, Solomon Islands, Tonga and Vanuatu. We focused on promoting the adoption and use of the 27000 Series, and really raising awareness as well, that was a big piece of the work too. At the end of the project, we published [a report](#) which has recommendations for further engagement and participation in each of the five countries. I'd be happy to share a link to the report as well for anyone that's interested.

Common Themes from Key Recommendations

	Develop National Cyber Security Strategy/Policy
	Create Cyber Security Working Groups/Committees
	Enhance ICT career paths and education
	Enhance ICT training and certification
	Develop community awareness campaigns



I've pulled out just a few of the key recommendations which were common across all five countries. Of course, they differed between the five, but here are some of the key common themes. Many of the recommendations related to further raising awareness on cybersecurity, and the role that standards play, whether it's through community campaigns, or more formal training and education programs. Another key recommendation was related to the development of national strategies, or policies, for cybersecurity, which might consider standards, and the role that they could play in supporting those policies. Lastly, it saw the establishment of working groups focused on the adoption and greater use of cybersecurity standards, to serve as the standards champions. So, at the end of the program there were driven groups to keep the momentum on the work.

I will leave things there, but definitely open the floor for questions and comments. Thank you.

William Tibben

Thank you, Torrin. That was really good. I know there's a quick question from Rajnesh, asking you about the report. If it's possible maybe to share that either through the chat, or even later on, if you don't have the details available at this point yet.

Torrin Marquardt

For sure.

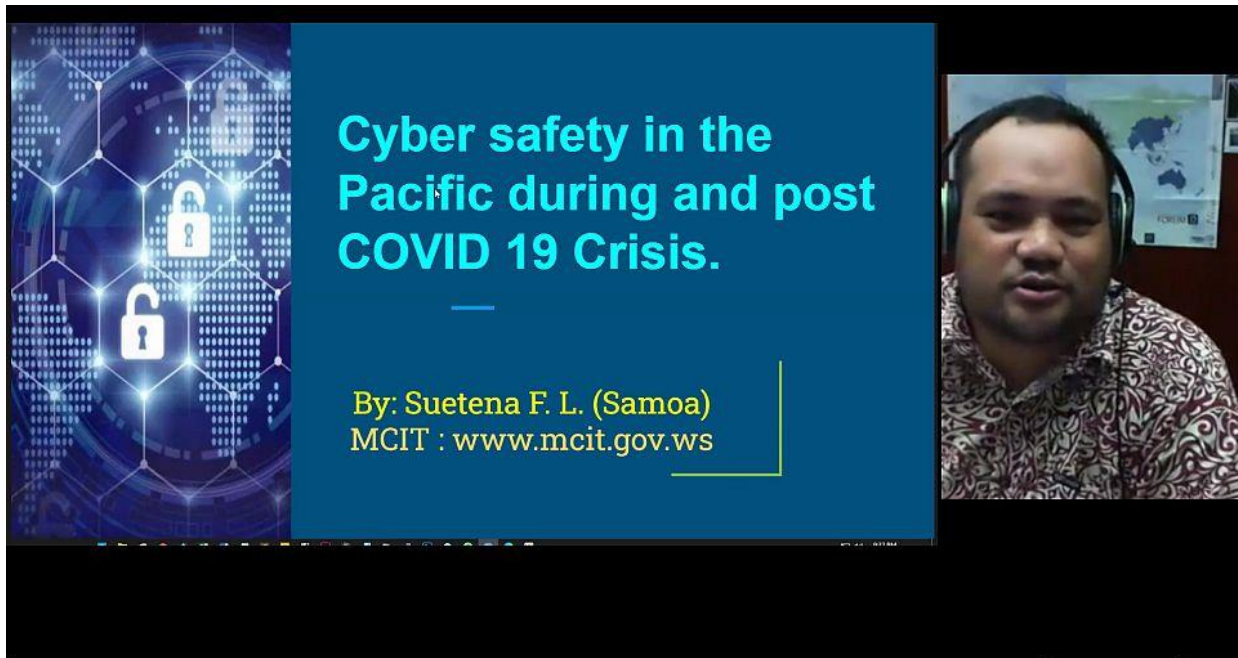
William Tibben

Okay. What we might do is, I know there are some questions coming through, but what I think we should do is probably just move on. Anne is just responding to some people, which is quite good. Thanks, Anne, for that.

Suetena Loia, from Samoa, the Ministry of ICT. I'll hand it straight over to Suetena. What I'd like to do is maybe get everyone to have their say, so that if we can leave time at the end for questions, rather than having too many questions now, and then having the last person not really being able to speak. That's how I'd like to try and do it. Suetena, you've got the floor, and I'm very interested to hear what's happening in Samoa.

Suetena Loia

Thank you, William.



@PICISOC #eTALANOA

Suetena Faatuuala Loia, MCIT

Internet Society
Pacific Islands Chapter

Good evening everyone, and good evening friends from the Pacific, and colleagues, I see some familiar faces, as well as some familiar names. My name is Suetena Loia, I am the Acting Chief Executive Officer for the Information Communication Technology Division for the Ministry of Communications and Information Technology, of Samoa. I'll just try to provide some overview of what Samoa has been doing in terms of pre COVID, post COVID, and during the COVID scenery.

Cybersafety : PreCOVID-19 (Normal)

- Awareness and Knowledge Capacity were in developments.
- Samoa had developed its Cybersecurity Strategy (CS) 2016.
- Child Sexual Abuse Material Filtering Policy (CSAM Filtering Policy) 2017
- Approval of SamCERT Setup 2019
- Approval of Digital Transformation Authority Setup (GoS) 2019
- Samoa Information Technology Association (SITA) 2019
- Developments in Digital Transformation saw the need to develop CS Support.
- Financial Institutions were already fighting Digital Cyber Crimes with increase financial fraud. Reviewing process of validation and increase financial awareness around Identity protection and trust circle verifications.
- Developments in Cybersecurity policies are in development.

Before COVID actually hit the world, Samoa was already engaged in developing its cybersecurity and cybersafety initiatives. From that it created awareness and knowledge capacities, in terms of programs and schemes throughout the country, with works from partners and in other avenues of support.

In 2016, Samoa had developed its cybersecurity strategy, and this strategy has been the pathway for all cybersecurity development, as well as cybersafety within the country. Through that, it had developed the Child Sex Abuse Material Filtering Policy, which was work from our sector, through the Office of the Regulator, and the Office of the Attorney General, in terms that it will be adopted by telco companies, as well as ISPs within the nation, to actually filter online content and other mischievous materials.

In 2019, the government of Samoa had approved the setup of a national CERT, and through that work in 2020, is now in the pipeline in terms of erecting this national CERT, as SamCERT. In 2019 as well, we saw the approval and the move forward of having a national Digital Transformation Authority, which will guide all national digital transformation projects, as well as producing standards and regulations for both public and private companies, in terms of standardizing technology and standardizing process, and standardizing all the work that is required to actually produce a digitally transformed country.

Also in 2019, the Samoa Information Technology Association was established. The purpose of this association is to assist the government, both in the private sector as well as the public sector, in


raising awareness in terms of utilization of technology, especially in the area of information, and improving cybersecurity and awareness in terms of engagements with communities, as well as other partners, in terms of producing a well-informed population of how to use technology online, and how to use technology offline, in terms of protecting the data and information.

We saw a lot of digital transformation that were happening, and the need to also develop cybersecurity support within the digital transformation was the other area that the government saw that required support, in terms of setting up the Digital Transformation Authority. At the same time, a lot of the other areas such as financing, and infrastructure, saw a lot of cybercrimes resulting from increased financial fraud. Through these increases banks and financial institutes review process in terms of validation, and increase financial awareness around identity protection and trust circus verification.

As well, in the works, the Ministry is working in terms of developing a cybersecurity policy, which will influence other current work that has been developed throughout the time, that cybersecurity has been one of the major agendas for Government to actually bring forth and to increase the awareness on.

Cybersafety : During COVID-19 (Good-guys)

- Cybersecurity Policy development Prioritised
- Awareness and Knowledge Capacity pushed through online Portals and Video Streaming Site.
- Development of Cybersecurity Guides and Materials.
- Digital WFH spiked saw the need to develop CS Support. Strengthening Collaboration with Partners locally and Regionally.
- Financial Fraud saw an increase , Financial institution push out warnings and awareness materials to combat this wave of attacks.
- Government Bodies prepared Cyber support plans for Full Digital and Remote work.
- Partnership Private Sector for supporting Free Safe SIMs, Online Educational Portals.
- Joint Coordination with the National Emergency Operation Center (Samoa) for online Safety.



**Everything is in
Hyper Drive**

In terms of the COVID, it has been something that has hyper driven a lot of these initiatives that the government has already planned for, such as putting the prioritization on the cybersecurity policy development, as well as increased awareness and knowledge capacity throughout portals and video streaming sites as well as television and radio. Development of cybersecurity guidelines,

and guides, materials, that are published online for various government websites such as this, is one of the terms that the Ministry of Communication has endeavoured, producing cybersecurity bulletins monthly throughout the whole year.

Through this attempt, a lot of the areas in terms of work from home have spiked. Collaboration with partners and local stakeholders in terms of improving this drive for a safer and better Samoa has been going quite smoothly at times, and not so smoothly at other times, but through COVID I think we have been able to manage those quite well.

We've also seen a lot of increases in financial fraud, spams, and people being tricked, financial attempts trying to take money from their bank accounts, and through online services. Many of these financial institutes have pushed out warnings and awareness materials, trying to combating these areas of attacks.

During COVID, as well, a lot of the government bodies have come together in trying to not only act in a national emergency, but to actually produce a digital plan, rolling out work from home plans ,and work from home security measures for employees, as well as customers, to actually produce the requirements for sustaining Samoa's operation while under lockdown. For these partnerships with the private sector, the telcos have seen free safe SIMs, and online education portal going up, through the assistance of SITA. As well as this, joint efforts both from the Ministry and the National Emergency Operations Center, producing online safety materials, as well as continuous radio awareness on how to be safe online.

Cybersafety : During COVID-19 (Bad Guys)

- Ransomware Campaigns increased
- Financial Fraud Campaigns increased
- Malware campaigns increased and vectors of infection been explored in terms of context of a country.
- Social Media and Online Account Takeovers
- Website defacement and Genuine Sites been used as watering holes for malware repositories.
- Cybercrime has become a business and are hiring professional people to create tools and infrastructure.



**Even the Bad
Guys are in
Hyper Drive**

In a general form, I think a lot of our colleagues have shared the same understanding. Even the bad guys have gone into hyper drive. You've seen a lot of increase in ransomware campaigns, financial fraud, malware campaigns from various vectors, and some of them are very creative nowadays, social media account takeover, website defacements. Cybercrime is becoming a business and are hiring professionals to actually create these infrastructures and tools.

Cybersafety : Post-COVID-19 (Cloudy Days)



The Road ahead is a long one

- We all need to wake up and know that everything is changing.
- COVID-19 has become a catalyst to Digital Change and Digital Adoption.
- This Catalyst have put all of us in Digital Space which has create a bigger pool for attacker to go for.
- Cybersafety not only be a personal need it will be a National Security Problem.
- Cybersafety will affect all areas of the Samoan economies
- Cyber is the future infrastructure of everything.
- Awareness will increase as new attack vectors increase.
- Community support from Educational bodies Industry leaders is vital to fight these new ways of attacks

The road ahead is quite long. We all need to wake up and know that everything is changing. COVID has become a catalyst to digital change and digital adoption. This catalyst has put all of us in digital space, which has created a bigger pool for attackers to go for. Cybersafety will not only be a personal need, it will be a national security problem. Cybersafety will affect all areas of the Samoan economies. Cyber is the future infrastructure of everything. Awareness will increase as new attack vectors increase. Community support from educational bodies, industry leaders, is vital to fight these new ways of attacks.

What's Next - Future Actions

- We all need to be creative with Cyber Safety Campaigns
- We need to Strengthen Legal and Regulation to include CyberSafety support in products and services that our business provides.
- We need to Build a cyber safety Culture that is second nature
- We need to Integrate cybersecurity and cyber safety in the fabric of our Pacific culture.
- We need to review operational process to include Cybersecurity and Cyber Safety as part of Organizational risk management.
- We need to work together on many levels to see this through in the days ahead.
- Digital Services is the future and we must build resilient and secure infrastructure.
- We must continue to strengthen Regional and International Partnership such as Pilon , PacSON and more.



**A Collective Effort for
sustaining everyone**

What's next for the future and future actions? We all need to be creative with our cybersafety campaigns. We need to strengthen legal and regulations, to include cybersafety support in products and services that our business provides. We need to build a cybersafety culture that is second nature. We need to integrate cybersecurity and cybersafety into the fabric of our Pacific culture. We need to review operational process to include cybersecurity and cybersafety as part of the organizational risk management. We need to work together on many levels to see this through in the days ahead. Digital Services is the future, and we must build resilient and secure infrastructure. We must continue to strengthen regional and international partnerships, such as PILON, and PaCSON and more.

Is it Possible



Is it possible to develop cyber security policy in the Pacific where the key metric of success is cyber safety?

YES

Q?

1. It Creates a Cybersecurity Standards
2. It will Influence new Laws in the Areas of Cybersecurity and Cybersafety.
3. It will strengthen Knowledge tools and as well as Cybersecurity Infrastructure.
4. It will open doors for a cybersecurity Industry which will enable for greater Cybersafety Support.
5. It will produce new talents and resources available in the region to greatly impact the sustainability of the overall Cyber Safety Agenda.
6. Consider Country Prioqrities / Local Laws / Level of Developments
7. Consider Unity of Local Law and International laws around Cybersecurity.
8. Supporting the Budapest Convention and other International support around cybersecurity engagements.

A question we want to answer: Is it possible to develop cybersecurity policy in the Pacific, where the key metric of success is cybersafety? Yes, it creates a cybersecurity standard. It will influence new laws in the areas of cybersecurity and cybersafety. It will strengthen knowledge tools as well as cybersecurity infrastructure. It will open doors for a cybersecurity industry, which will enable for greater cybersecurity, safety support. It will produce new talent, and resources available in the region, to greatly impact the sustainability of the overall cybersafety agenda, considering country priorities, local laws, levels of development, and considering the unity of local laws and international laws around cybersecurity, supporting the Budapest Convention, and other international support around cybersecurity engagement.

Thank you : #Cybersmart-Pacific

- Use Strong Passwords
- Think before you Click. Post. Type
- Make Secure Choices
- Protect your Devices
- Browse Wisely



On that note, I would like to thank everyone for tuning in. And here are a few things that you could do in terms of staying safe online and be cybersafe. Use strong passwords. Think before you click, post, type. Make secure choices, protect your devices, and browse wisely. And, as far as the October theme for PaCSO, Cyber Smart Pacific has been a campaign that we have pushed out. And this is a video. I would kindly request if I could actually have time to play this video for everyone?

Video playing

See the many advantages cyberspace offers and our economy and quality of life are better for it. However, as we enjoy its benefits, we also recognize that it threatens us in a variety of ways. Everything around us is connected digitally. What you see may not always be true. Who you think you know may not always be who they appear to be. The question is: Are you safe online? Every day you may come across unknown attempts to jeopardize your data, your devices, and your personal identity. Sometimes a casual peek is really snooping. Sometimes sharing information too often may result in critical private data being made public. Sometimes a lucky find can lead to bad luck. Even visiting a website can lead to unnecessary sites. Today, cybercrime causes huge problems for society, personally, financially, and even matters of national security. To avoid getting these threats, use strong passwords, think before you click, post and type, make secure choices, protect your computers, protect your devices, browse wisely, protect ourselves, be cybersafe.

William Tibben

Thank you very much, Suetena. It's great to see all the work that Samoa has been doing. In a sense, you were kind of very well prepared for the COVID in a number of different ways. I was thinking that, certainly with all the work that's been done since 2015, with the cyber strategy and cybersecurity strategy, and digital transformation, has really been paying dividends now. Thank you very much.

Now we're going to move to Klee. Klee from CERT New Zealand

So, Klee, yeah, the floor is yours. Take it away. Thank you.



Klee Aiken

Thanks, William, and kia ora, everyone. I'm Klee from CERT NZ.

Cybersecurity and COVID-19 is quite the expansive topic. I'm going to touch very briefly on a couple of issues. If anything catches anyone's eye, we can dig into it a little bit more through the conversation.

I want to start with what we're actually seeing. I'll just share a couple of stats from New Zealand, it's based on the reports that CERT NZ has been receiving. Based on the conversations that we've

had with our Pacific partners across the region, a lot of the trends that we have here in New Zealand -- while the numbers might not be exactly the same, the trends are quite familiar, and quite similar to what a lot of the other countries in the Pacific are seeing. One point is really just in the rise of reports of incidents that we're receiving. In 2019, we had 4740 reports, and then the first half of this year alone, we already hit 3120 reports. The highest month was a huge peak in April, where we had 820 reports just in that one month. It correlated directly with when New Zealand entered Alert Level Four, which was the highest level of lockdown that we reached. So, it's unsurprising that there's likely a linkage between that alert level, and the rise in the reports, and potentially the rise in incidents as well.

The range of incidents that we're seeing covered the whole board. Some major things that we saw included malware and ransomware. I really want to highlight that right now, because we're actually seeing quite a new wave of Emotet. If anyone's been reading the news of what's happening in the US with Ryuk, that's targeting hospitals at the moment. That's not necessarily something that we've have any reports in across the Pacific, but Emotet is something that we've been seeing quite a bit of across the regions. So, it is something to be aware of.

While there's, like I mentioned, a huge range of incidents in the region, the real driver of the growth, as for CERT NZ, similar to some of the points that the other speakers have already pointed to, were scams and fraud. Between quarter one and quarter two, we saw 230% increase in scams and fraud, that spike largely driven by extortion and blackmail. We also saw a gradual but sustained increase of scams related to buying and selling online. That's a huge trend, and quite important to take note of, because it's really impacting the way folks have shifted the way they're working, shopping, and trading online.

This is something that Suetena mentioned in Samoa, but also in previous conversations across the Pacific that we're seeing. The financial markets authority here in New Zealand actually issued a report, back in May, specifically highlighting some targeted campaigns focused on the Pacific communities here in New Zealand. We've received reports that these are also carried over into the Pacific. We were able to share those with the specific islands that were mentioned in the reports.

It's a challenging picture. I don't want to paint something a little too bleak. I know we've been pointing out a lot of the challenges that we all face. It's also a big opportunity, where there's a lot more attention being paid to the importance of digital connectivity and digital technology. It's a trend that was already started. One thing, at least for us on the practitioner side, is very important is it has increased the attention and focus on the security side, and the security aspects of digital

transformation, which is a very important dimension. So, it's an opportunity, while it's a challenge, it's a huge opportunity for us to take strides forward on this space.

But, what do we do about it? Obviously, there's a whole bunch of different approaches that we can take. The most important thing is to understand how diverse cybersecurity issues are. It takes a whole range of actors, each actor with different roles, different responsibilities, different capabilities, and different interests. There's no one size fits all solution, and there's no one organization that's going to be able to solve these challenges. It really takes everyone working together. It's actually a really nice reflection of that, in terms of the diversity of the panel today, but also of the audience. It's really great to see folks, not only from the technical area, but also decision makers, policymakers, everyday users, businesses, both big and small, as well as the incident response community, and others, coming together, because it really is going to take everyone applying different approaches, but working together, to rise to these challenges.

I do want to touch a little bit on the Incident Response Community, because obviously coming from CERT NZ, that's kind of our home, or where we're most comfortable. As I mentioned, we're only one piece of the puzzle, here in New Zealand, and CERTs across the world are only one piece of their local and international puzzle as well. I do want to highlight what we focus on here at CERT NZ. Our mandate has five main pillars: incident response and triage, situational awareness and information sharing, advice and outreach, and awareness raising, international collaboration -- and our work with the Pacific is particularly important for us as CERT NZ, and it's great to work with the Pacific community -- and coordination of serious cyber incidents.

I'm not going to go in depth into any of those, but if we want to dig into it a bit deeper during the questions and answers, we can. What's really important, is what it boils down to. That's coordination, building relationships with diverse stakeholders, domestically and internationally, and building partnerships that are really focused on doing work, solving the challenge, solving the incident. What it really takes is an underpinning and a foundation of trust across your community, and trust with stakeholders. This is something again, that happens both domestically and internationally. We rely very much on the different network operators in our community, chambers of commerce to raise awareness, other organizations in the internet ecosystem. For us, we work quite closely with Netsafe, that focuses a lot on the safety side, we work very closely with Internet NZ, and the .NZ domain names that have their space in the Internet community. Within government, we're working with other agencies, the National Cybersecurity Center, Department of External Affairs, and all across the board, even foreign affairs, to address some of these challenges.

It's important to build those linkages, and it's great to see those similar linkages starting to build up and strengthen in our neighbors as well. I know Suetena mentioned SITA, in Samoa, is a key partner growing, and I know Saia is on the call as well. In Tonga they're doing great work building a cybersecurity community there. TWICT is a great group that's really taking the lead, again on the cyber safety side, recently. Internationally, as well, we're really dependent on sharing information, and building partnerships, and coordinating, not just for incident response, but also to share best practices and learn from each other. As Suetena hinted at, with the mention of PaCSON, there's a really great opportunity to plug into some regional networks that exist, and are developing. This E-Talanoa Initiative, as well, is a great way to share information, and learn from each other's experience.

I did want to touch on one last point before we move on. That is awareness raising. This is just a really great example, and the most recent example, of how we can work together as a region. While they can be the most challenging folks to reach out to, they are the most important, and that's the users. They're a key audience, because that's really the interface of humans and the machines. That's where a lot of the challenges can take place, but where a lot of the solutions, where really small steps can add up, and solve a lot of the vulnerabilities that we're facing.

Suetena has already mentioned this, one of the big projects that we worked on recently was for Cyber Awareness Month, in October, so it's just wrapping up this month, and that was the Cyber Smart Pacific Campaign. The group came together, the incident response points of contact across the region, under PaCSON, proposed a whole bunch of different themes and titles, and we came up with Cyber Smart Pacific, Step Up your Digital Safety and Security. We shared four key lessons, the lessons that we've been using here in New Zealand for the last couple years, for Cyber Smart. That's using a password manager, deploying two factor authentication, updating your software and devices, and checking your privacy settings. These are four relatively simple steps, but they can go a long way to solve the majority of the challenges that many of us face on the cybersecurity side. It's really important to be able to share that with each other, and work together to develop this campaign. You saw what Suetena, and the team over in Samoa, did. I know a lot of the other islands and representatives here -- Kensly might share, what they've done in Vanuatu, and then some of the other folks on the call might be able to speak up on the work they've done under the Cyber Smart Pacific campaign.

That's just one example. It's, I think, a really nice example, it's the most recent example, of how we're able to share, and work together, to take these small steps, that have a big impact in the long term, to build a more resilient community, and a stronger security community, that can build up the ecosystem. We can definitely unpack some more ideas on what we have done as a group.

I'd definitely be keen to hear, not only from the other panelists, but also everyone on the call, different proposals and different ideas on new initiatives that we could take on, different ways that we could work together, build capacity, and do some cool stuff that'll help hopefully turn around some of these worrying trends that we're seeing in terms of cybersecurity.

William Tibben

Okay, thanks a lot Klee, that was fantastic to hear about what was happening in New Zealand, particularly the connection with Pacific Island countries there, and being able to feed some of that information back into the Pacific Islands. Thank you very much.

Now, our last speaker, before we throw the floor open to general discussion, is Kensly, who also comes from a country which has been very proactive in terms of ICT policy, particularly. I suppose it's no coincidence that they're kind of right on the ball with another CERT. So I'll hand it over to Kensly to tell us about what's happening, what's been happening, in Vanuatu.



@PICISOC #eTALANOA

Kensly Joses, CERT VU



Kensly Joses

Thank you, William, and good evening, everyone. I hope you can hear me clearly, excuse my voice, I've been down with the flu for the last three days.

I'm glad to be part of this discussion. Cybersecurity in COVID-19 and post COVID-19. There's lots been done over a cybersecurity space, especially in various countries, internationally, globally, and within our Pacific region, and I hope in various Pacific Islands as well. In terms of what Vanuatu

has been doing so far, CERT Vanuatu is a newly CERT established in Suva University. This will be the third year of existence. And we are glad to work along CERT Tonga, CERT New Zealand, ACSC and other PaCSON members. For us, on the Pacific Islands, who are part of this conference this afternoon, please make an effort to join PaCSON, a very active network, very active community in addressing cyber security issues within our region.

CERT Vanuatu existence comes into effect via our National Cybersecurity Policy in 2013, which states the existence of a national CERT, and ends in a CERT Vanuatu existence in 2018. Klee was fortunate to be part of the launching activity for CERT Vanuatu at APNIC. We launched with two main objectives. That is to respond to cyber security issues or threats within Vanuatu, and to promote cyber security awareness within Vanuatu, and to serve as a point of contact for cybersecurity in Vanuatu. Not only Vanuatu, but to collaborate with the region as well.

We've been doing a lot of awareness work over the last few years. Recently, we've been hit by COVID-19. I presume all economies have the same, the same difficulty. In terms of small island nations, we know resources are very limited. When COVID-19 hit, Vanuatu, was not badly hit by COVID, we are still COVID free. But there are precaution measures that we got from the instructions from the SoE, the State of Emergency, which the government has put in place, with clear instructions for things like social distancing. This has dramatically affected the services for organizations and businesses in Vanuatu, and the government as a whole. CERT Vanuatu is still under the government, at the Prime Minister's office.

During COVID-19 we've worked together with other government agencies, to put up a readiness plan, to move with our readiness plan, in case of a worse scenario, if there is a case in Vanuatu. What are we going to do? This means we identify key government essential services that need to be operated, need to be running. We have to look into equipment policies, with the worst case scenario, where employees were to work from home, how will the government look into budget, to purchase new equipment, or if the equipment in the offices can be relocated to the homes, things such as creating new fibre connections. These are some of the things that we work together with the government agencies, to put up a readiness plan to address the worst case scenario, if there is a COVID case in Vanuatu.

COVID also sort of helped us, the citizens, in a way that the businesses tend to step up the security approaches, and the security practices. Most of the services have already been saved to cloud services, they are starting to use cloud services for example, the education sectors.

When the COVID hit, when the COVID virus came out, the Government, the Ministry of Education a notice for closing all schools, [and has also been in collaboration with CERT, and another private organization, to help set up a Moodle for schools. Currently schools in Vanuatu are already using Moodle. These schools are secondary schools, not all, but a good percentage of them, are using Moodle at the moment. That is something that COVID has brought, which we haven't seen before. We predict that these changes will come, but not as fast as what is happening.

Government users, and not only the government users, but we've seen organizations switch from normal meeting to online conference meeting, using Zoom. We're aware of the security threats and vulnerabilities in in Zoom, we've put out an advisory to our constituency, Internet users, to organizations, in relation to several vulnerabilities in Zoom.

We have also seen organizations moving into seeing the importance of collaborations. The approach we took in Vanuatu is to take a multistakeholder approach, where we invite the different stakeholders to work with each other. Stakeholders include our our ISPs in Vanuatu, the regulator office, the police. the Vanuatu Internet Governance Forum. We recently, post COVID-19, we signed a multistakeholder MoU, memorandum of understanding, to collaborate in all cyber security issues and cyber safety issues, to address those issues within the region.

We've seen a lot of social issues coming up recently, with the trends going on, on account of COVID. We've also seen an increase in online presence of Internet users in Vanuatu. There is a huge increase in online presence. I believe it is because people are relying on Internet for services. That also makes us think about the security of the users. More users will be vulnerable. We've seen similar trends of others, as mentioned by some of the other Pacific Islands, and I believe every economy has seen the same trend of attacks happening. We are able to put figures to the attacks happening in Vanuatu, and these are successful attacks. What we've seen mainly online scam, fraud, and also cyber enabled activity, which are going on in Vanuatu. Some of the scams are successful, and we were able to put figures to that, and these are our citizens, who are users. We've seen business email compromised as well in Vanuatu. Organizations in Vanuatu lose a huge sum of money.

How do we address the issues? We are moving in a way that we want all our stakeholders, all the businesses, to collaboratively work on addressing cyber security issues. One of the things we realized during COVID-19 is that we haven't put any strategy in place to address cyber security issues. Therefore, we are working on our cyber security strategy, which we are hoping to launch by the end of this year.

These are some of the efforts that we have put in Vanuatu. Another one that we are hoping that it will come into existence is our cybercrime bill, which is ready to be tabled in to Parliament next month. We are hoping that this can pass by the Parliament, and then we can have a cybercrime law to serve us to prosecute any crimes, or any offenses committed within the boundary. And hopefully we can be part of the Budapest Convention, and other conventions, where we can work together in addressing those social issues further.

Since Vanuatu embarked on the National Cybersecurity strategy development, we have done various national consultations for our cyber security strategy. This we have completed last week, which we are really happy, and our strategy is now at the drafting stage. We are waiting for the review, and then hopefully we can have something in place where we can follow for the next 5 or 10 years down the road, to address our cyber security issues in Vanuatu.

We are also part of PaCSO, as I mentioned. We have October as our cyber month. We collaborate in Cyber Smart Pacific campaign in Vanuatu as well. We've put out posts via our social media reach, to our citizens, we've created flyers, and we also produced two short awareness videos, one addressing the use of two way authentication, and another one on phishing attacks and online money scams.

Into the future, we will only see an increase in cyber threats. There will be breach after breach, despite all the security necessary put in place, the monitoring equipment, and all this, we will continue to see a rise in number of threat actors around the world, internationally, within our region, within our own economy. But I will echo the words of the various presenters, I believe in, we believe in collaboration. Collaboration is the key to our success in Pacific. If we can collaborate in every level, then I believe we will have a safe Pacific. Thank you very much.

William Tibben

Thank you Kensley, that was great. Thank you very much.

Okay, well, now's the time to start thinking about questions that you want to pose to the audience.

Does anyone have any questions that they want to jump online straightaway?



William Tibben

What I'll do is, I'll just pull up one of the questions that was posed earlier on, which I think was mainly to Anne, but I think, probably is a good one just to throw out to everybody, which relates to young people, in terms of how to engage young people. At some point, I think Suetena talked about education as an important aspect, in terms of developing a comprehensive cybersecurity approach, which promotes cyber safety. So, I'll just throw that question out, are there any kind of ways that young people can really participate in these kinds of initiatives to promote cybersecurity?

William Tibben

Torrin? Does Standards Australia have any kind of outreach activities to young people, to each them about standards?

Torrin Marquardt

Yeah, that's a good question. I understand my answer might be a little different than how the others might answer it. I think in the standards world, a big thing that we're trying to see is the integration of standards education for, say, universities and education at that level. Often for engineers, other technical areas of work, standards is not part of that education. Around the world, that's something that we're hoping to see increase. As well, in the actual development of the standards, it's really important to have a really diverse group of people involved. That doesn't just mean different countries, or different genders, different ages is just as important. That's

something that we're working hard to do, is get the next generation involved, and in the region as well, are looking at ways that we can get younger people more involved in the standards process, and understand the value.

Torrin Marquardt

Standards are something that, when everything's working fine, they're working well, they're invisible. It's when something goes wrong, that, you notice them, and it's when they're in place, and things are working smoothly, that they're at their best.

Torrin Marquardt

That's a roundabout way of answering it, but I think it's important to have not only the awareness piece for young people on the importance of standards, but then also have greater involvement in how they're developed too.

William Tibben

Thank you. Anne, I think the question was directed at you. Do you have a response to that in terms of Fiji?

Anne Dunn-Baleilevuka

I just wanted to add on -- I think I had answered separately to the individual who asked -- but just to add on to that. Having a standard almost, but I realized that you're not in the educational space.

Anne Dunn-Baleilevuka

It was really interesting to see, for Fiji, that students were very interested in this cybersecurity, cybersafety, space, even if they didn't fully understand what it meant. Every time we did school awareness, or community awareness, they were very much engaged in what the process looks like. And so I definitely think that there's room for engaging young people here. Young people can participate at really different levels. You have policy levels, where individuals are encouraged to submit whatever their thoughts may be to the relevant ministries, or at least to the commission, as well. We had gone to a university a few months ago, where the university students ended up submitting thoughts on what they thought of cybersecurity, and particularly for cybersafety in Fiji, because there's different legislations that are up for review in the next couple of months, and so they were able to get engaged in that manner.

Anne Dunn-Baleilevuka

There are also public consultations that young people can get involved in, and even different companies are looking to engage young people, on a placement or volunteer basis, with the

different companies that are in the country. There's definitely spaces to get involved. I do know that Save the Children, here in Fiji, is also doing a project, and they're involving particularly young people to get their perspective on what digital cyber hygiene, cyber safety looks like for them, and what they think that is. So, there's different NGOs, there's different CSOs in the country that are having their individual pocket exercises, and they're really wanting young people to get involved, because that's the generation that grew up with these technologies. And so, particularly here in Fiji, where there's a bit of -- oh I'm sure that they have it in other countries as well -- but there's a bit of a gap in terms of the understanding of technologies, and so you have a generation that didn't necessarily grow up with it, but is using it for work, and for these types of things. And then you have an entire generation that's growing up with it, being given to them at like the age of one or two for the simplicity of just keeping them quiet, I guess, so just entertained for a certain amount of time, to be able to do something.

William Tibben

Any others want to jump in on that particular question? No? Well, I've got another question that relates to increased delivery. It kind of talks to what Kensly was talking about in terms of Moodle. There was a question from Kanesh asking with online learning and internet being delivered into schools, does any country have policies or frameworks for a safer online experience?

I'll throw that to you Kensly, seeing that you spoke about it.

Kensly Joses

In Vanuatu we have our Ministry of Education, they have a cyber security policy. I believe that most of -- all institutions adhere to the policy, but we are on our outreach awareness to the schools. We spoke with the principal, and we encourage schools to have ICT, or cyber security policy as well, developed for the institutions. But, in terms of nationally, our Minister of Education has put out a cybersecurity policy for the Ministry, part of the policies covers cyber safety issues as well. So, I hope, that is from Vanuatu, I hope I answered the question.

William Tibben

Thank you. Yeah, Suetena, do you have anything to add from Samoa on such?

Suetena Loia

In terms of education?

William Tibben

Yes, yes.

Suetena Loia

At the National University they are experimenting on a cyber security culture, where through other university, they are posting a lot of the awareness in terms of how to be safe online, how to pick out what could be online, like hoaxes that could actually get them in trouble. Those are some of the things that they are experimenting on. They've been doing that during COVID. SITA is part of putting out those online portals. They also are teaching the four attributes of Cyber Smart Pacific, which is using a password manager, and maintaining your security online, checking your privacy settings, and stuff like that. So, not only has SITA been pushing those digital transformation platforms, they've also been training those security and safety awareness campaigns together. From the educational perspective, I think it's building that cybersecurity culture, and then that culture becomes a part of students' habits in terms of actually executing and getting online for those type of things.

William Tibben

Okay, thanks. I noticed Klee has been quite active on the chat. Do you have anything else to add to that?

Klee Aiken

I guess some folks are sharing some resources. So, I shared Netsafe, which is an organization here in New Zealand that looks after cybersafety. They've actually been around quite a bit longer than us, and they started with a focus on the education community. That's a little bit more of their space than CERT NZ space. I would definitely point to them for good resources. Torrin shared Cybersafety Pacifica which is, I guess, a law enforcement community across the Pacific. Definitely plus one, Torrin. Saia shared Get Safe Online, which has some resources, and Anne did as well, as well as the Online Safety Commission.

The reason I'm stealing everyone's links and sharing them is, it is a little bit outside of the CERT NZ core space, especially the youth angle. But if we're talking the older end of the youth spectrum, I definitely encourage what Suetena was talking about there, about building that community. There are a lot of open communities, and E-Talanoa is kind of developing into that as well, where cyber issues are being discussed. SITA is one with a lot of that professional angle. There's things in Samoa and Vanuatu, with VAN IGF, and in Tonga, and all over the place. These communities can be a great place to not necessarily have formal training, but really get introduced to the issues, and be able to meet other people working in the space. Getting that kind of practical information sharing and experience sharing can kind of be the best way to build that expertise.

Kensly Joses

William, if I can add on to my response earlier. We have the Vanuatu Internet Governance Forum, in Vanuatu, where a lot of the activities revolve around education, and they have been very active with the institutions around in Vanuatu, to help them in those kinds of areas. One thing that I forgot to mention earlier, is, within our cybersecurity strategy, the different approaches and the priority areas, our key priority areas, and how the response to those key priority areas, we've taken into consideration, as well, those things such as helping institutions with policies, especially schools and other government institutions within the country. This is something that we are focused on. One of the key priority areas for our national cyber security in Vanuatu strategy is capacity building, cybersecurity capacity or capability within Vanuatu. That is one of our key priority areas in our National Cyber Security Strategy. Thank you.

William Tibben

Okay, thank you. Now, we're kind of getting towards the end. I think there's one question which is probably relevant here, is the one that relates to a regional framework, cybersecurity framework. Is that something that's being actively pursued? I'm just trying to find that question. Here we go. It's actually from Cherie, I think, or possibly Tim. What are the next steps for pushing for a regional cyber security standard? I suppose the first question I'd like to ask, is something like that necessary? And then the following one is, it's a question for Torrin, but I'll throw that out to everyone as well.

Torrin Marquardt

I can answer that first. It's a good question. I would agree with what you were saying just then, Will. I would say it's actually not necessary. The point of having an international standard is that, even beyond the Pacific, experts from all around the world have come together and agreed on what best practices for cybersecurity, so they've kind of done the hard work for you. So, yeah, I would say that the work is already done, and the international standard would be the best place to start.

William Tibben

Okay. Does anyone want to disagree with that? And let's have a bit of a controversy to kind of finish things off.

Klee Aiken

This isn't necessarily specifically about standards, but in terms of the regional approach, I think there's space for all levels of the approach. A regional approach like what we're doing here, E-

Talanoa, what Cyber Safety Pacifica is, what PaCSON, is what PILON is, it's a really great way to build a network of like-minded folks who can share information, best practices, and help each other through different challenges. But you also need to have that local layer underneath it, with a strong local community, strong local organizations, to do the work on the ground. They can be mutually reinforcing, and each play different roles there. Those can, in turn, also plug into that international picture. So, while there isn't need necessarily for something like a formalized regional this, that, or the other, there's definitely space for the different layers, and different scopes, to all coexist and mutually reinforce each other.

William Tibben

Okay, thank you. Any others want to chip in with an idea there?

Okay, there might be....

Now I'll hand over to Tim Tuisawau, who's been dutifully taking notes. Tim's actually the lead for the Special Interest Group in PICISOC for cybersecurity. So, I'm interested to get some perspective from Tim as to what he thinks about what he's heard tonight, and where we go to from here.



@PICISOC #eTALANOA

Timoci Tuisawau, HFC Bank



Timoci Tuisawau

Thanks, Will. Well, I think it's been a very good session. We've got various perspectives, as mentioned before, both from the policy, with the Commission and the government perspective,

with someone counterpart have been his presentation. Also from a standards perspective with Torrin, and then we come down to the CERTs. I mean, these are the guys that, you know, sort of join the dots and check the packets and all these sorts of things. We've got various layers. As mentioned previously by Klee, it's not just an individual sort of approach, it has to be not only a multi-layered approach, but one that's done at various levels. I think with the panel that we have tonight, we've addressed that as much as possible, getting the views from various sectors of the industry, in terms of cybersecurity, cyber awareness. And I think, as mentioned by Loia in his presentation, in order to answer the question of whether cybersecurity can be a measure of cyber awareness, at the end of his presentation, he said yes.

With COVID, etc., that's happening, I think everyone is of the same view that the world has changed, and it's never going to be the same. The push to more online resources, online collaboration, etc, has just accelerated over the past few months. Just from my experience here in Fiji, a lot of things that we thought would take 6 to 12 months before we got there, actually happened in a very short period of time. The whole world is moving at hyperspeed, so to speak, towards online collaboration, and digitizing resources, and clouds, and things like that. But, as mentioned by Klee and the CERTs, on the other hand, you have other guys that are also enjoying the opportunity, where people are getting online, not being fully prepared for this sort of cyberspace, and you have these bad guys out there that obviously are going to take advantage.

It's very important, as put forward, I think the common message that came out was, there has to be collaboration, not only vertically, across the region, but horizontally within our own spheres of operation. I think E-Talanoa sessions like this just helps to create that awareness, and to help people network with each other. Just looking at the number of people that have come online today, I think there's about 23 people on this session, which is pretty much 23 people who have been introduced to each other through a 90 minute session. To summarize everyone's contribution, I think it's been a very valuable session. I've actually written down like four pages of notes. I probably won't be able to go through it all at once. But, in sort of in a ballpark sort of summarize thing, that's it. I can probably type it out, and provide it if people really want the notes,

Thanks, Will.

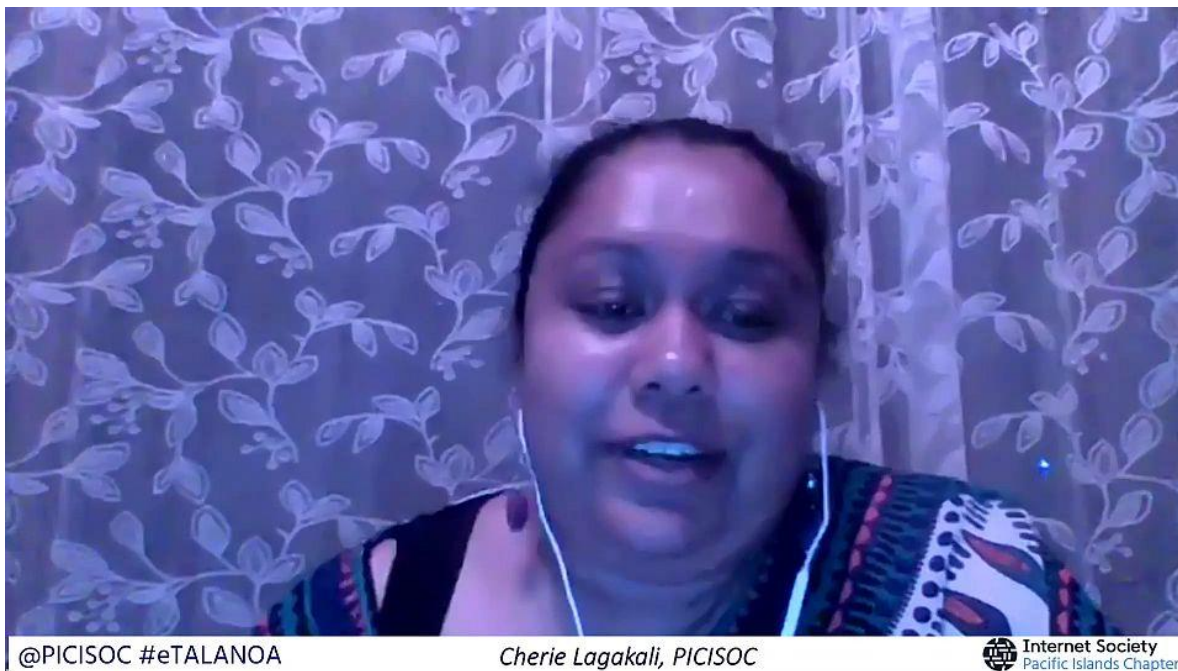
William Tibben

Thanks, Tim. I was wondering who's gonna do the summary? You just volunteered yourself, I think. Anyway, I think everyone's time is valuable. I really appreciate everyone being here and participating. The questions have been fantastic. Presenters have provided really good insights into what's happening around the region, so I'm really thankful. Thank you everyone for your

participation, it's been great. Also, thanks to Cherie and Tim for organizing a lot of the stuff behind the scenes. This must be the first PICISOC Zoom. I'm not, I'm pretty sure, maybe is that is correct? Cherie?

You just can nod if you like, if you don't want to speak.

It's gone off fairly smoothly, I think, really. I think. So congratulations to both of you. And this is the last opportunity if you want to, well, it's not the last opportunity, but certainly a good opportunity. If you'd like to maybe make contact with people and exchange notes. I think Tim's really summarized things very well. Would you like to say a few words Cherie?



Cherie Lagakali

No, Tim, I'm good, thank you. Thanks, everyone for joining tonight. We're looking at more cybersecurity related topics, but Will and Tim will be in touch through the mailing list. If you're not on our mailing list, please join to get in touch with us on this. Thanks.

William Tibben

Okay, well, thank you very much, everyone. It's been a great session, it's really good to see everything that's, I mean all the positive things that are happening and I agree with Tim, in terms of, I certainly would agree in terms of things that we thought would take months or years to achieve, have been achieved in very short periods of time. I know from my own perspective, having to teach and doing, we had to virtually transfer everything from face to face to online

within about three weeks. That was amazing how quickly we managed to do that. Like most of us, I think we probably spent a lot of time, weekends, nights, certainly put in a lot of overtime, which we probably weren't paid for. But anyway, we certainly learned a lot.

William Tibben

Anyway, thank you, everyone. Thanks and we look forward to making contact certainly on PICISOC list, and also LinkedIn, that's a great way to exchange details. Thank you very much, everyone. And we'll catch you some time in a later E-Talanoa session. Thank you very much.

Timoci Tuisawau

Thank you