GOVIS CONFERENCE - DIGITAL RESILIENCE

16 JUNE 2023

TE PAPA TONGAREWA AND ONLINE

The following was taken as a live transcript during the conference, by Katherine O'Brien from Mercury Transcripts using a specialist stenograph machine. It is supplied by GOVIS as-is, with only some very light proofreading, formatting and editing. We apologise for any errors or omissions.

Table of contents

9:00 - 9:15 am: Mihi whakatau **2**

9:15 - 9:30 am: Welcome and Conference Opening **2**

9:30 - 10:15 am: Building Cyber Resilience: 5 Things you can do Today **9**

Q&A - Building Cyber Resilience 21

10:15 - 10:45 am: Morning Tea **24**

10:45 - 11:25 am: Security and Sovereignty in the Cloud **24**

Q&A: Security and Sovereignty in the Cloud 35

11:25 am - 12:00 pm: Institutional Resilience - From Customer Service to Crisis Recovery **37**

Q&A- Institutional Resilience 44

12:00 - 12:40 pm: Lunch Break **49**

12:40 - 1:10 pm: Oceania Stream: Lightning Talks - Resilience in IM **49**

Evolution or Extinction? The Choice Facing Information Management - A Manifesto for Change 49

How Can we Apply Digital Preservation Principles to Help Organisations be Digitally Resilient? 55

1:15 - 1:45 pm: Oceania Stream: Digital Resilience in Papua New Guinea: A Judiciary Case Study **58**

Q&A: Digital Resilience in Papua New Guinea 66

1:50 - 2:20 pm: Oceania Stream: Lessons for Public Sector Reform from Australian Robodebt Royal Commission **68**

2:25 - 2:55 pm: Oceania Stream: Digital Resilience Lessons Learned from Disasters **78**

Q&A: Digital Resilience Lessons from Disasters 83

2:55 - 3:30 pm: Afternoon Tea **86**

3:30 - 3:35 pm: Ice Breaker Activity **86**

3:30 - 4:10 pm: The Chiefs Talk Digital Resilience **87**

Q&A: The Chiefs talk Digital Resilience 98

4:10 - 4:45 pm: Cyber Security in a Broken World **100**

Q&A: Cyber Security in a Broken World 108

4:45 - 4:55 pm: Conference Closing **111**

9:00 - 9:15 am: Mihi whakatau

- **Taranaki Whānui**

>>Kaumatua: Kia ora. (Te reo Māori). (Môteatea). (Te reo Māori). Hello, we're flash, we can speak two languages now. My name is Connor, I'm here on behalf of Te Atiawa and Taranaki Whānui, mana whenua for this part of te upoko o te ika, the head of the fish, I've been asked to come in this morning to open up your kaupapa for the day today so it's smooth sailing, and to welcome call of you who have come from outside the rohe, welcome, welcome.

Within my kōrero I touched on a couple of things, first acknowledgment to the ones who couldn't be here, the ones that have passed on, then I started over, you know where the mouth of the fish is and the ferries come in and out, over there we start our boundaries, it follows up all of these maunga all the way to Remutaka, all the way back down, over to a place called Rimurapa and back around to Turakirae. This outline's almost like an awkward triangle and that is the Taranaki Whānui, that's my people.

Welcome to Te Papa. Right now you're sitting under the protection of three maunga, so you have Matairangi which most people know as Tangi-te Keo, but its original name is Matairangi. You have Pukeahu which is up where the war memorial is and you have Ahumairangi which is back over behind parliament. But welcome. I hope you have a lovely day today. And all the best, I am going to be handing over to Mick. Kia ora.

9:15 - 9:30 am: Welcome and Conference Opening

- **Mick Crouch, Chris MacDowell**

>>Mick Crouch: I love it. Thank you Connor, that was fantastic. I feel both grounded and more nervous and excited than I was before at the same time, so thank you so much for that. Thank you all.

Hello my name is Mick Crouch, I wear many hats. I'm the GOVIS president and I'll be speaking to you on their behalf. I'm also the -- I also work at DIA at Archives New Zealand. But here I'm here to talk to you, I get the pleasure of doing the toilet speech. It actually says toilet speech.

One of the things I would like to say is thank you all for coming. Thank all of you here in person and online. Dan how many people do we have online at this the point? 18. Before Covid we probably couldn't do a hybrid conference like this, but now this is kind of expected. 18 people online is a fantastic start. So I'd like to say hello and welcome to all

the people online, to the people who are working from home as well as working in the office, and all of you. It's actually wonderful to see you all here, so many good friends, familiar faces, so many people here ready and excited about the day.

I'm also hoping that the whales come back. I'd missed them. A couple of days ago there was a couple of Humpback whales in the harbour. When I was a kid the blue whale was my favourite animal, it was the biggest animal ever. Anyway, the toilet speech. Welcome to Te Papa. In the case of an evacuation, there should be a slide. We know what to do in case of an emergency, drop cover hold, follow the directions of the wardens and assemble outside, that's Te Papa, that would be the Circa building. Of course if you're watching this from home or from work, you'll have your own emergency procedures.

The toilets are down the hallway around to the left, there's a men's room and a women's room there. Again if you're at home take care of that yourself. I'm trying to be inclusive to the audience who's not in the same room with us. Those who couldn't make it in person, right?

Mobile phones, everybody has a mobile phone, leave it on as you wish. If it's loud it can be funny when every watches you picking up your phone, so your appetite for embarrassment will dictate your actions there. There is a WiFi that's available here, it comes up straight if you want to do the WiFi, the password is events. It's on the back of your card, thank you Hayley and Raynor for that there is a Slido app that we're going to be using, Chris will talk more about that.

A bit about GOVIS in general, this is unusual, we've now done two one day conferences in the same financial year. Normally we would do one in June and it would be a two day event, this year we've done two one day events. We're trying to get our feet back into it because of Covid we didn't do this for a while, so we needed to -- is that someone's mobile phone? Really? Anyway, so we've been getting our feet back underneath us.

GOVIS, what is GOVIS? You're here at a GOVIS conference which is great, but GOVIS has been around for 30 years in some form or another. It started off as government information systems managers form is 1991 where they sat around and talked about exciting hinges like L DAP. Did LDAP exist in 91? Everyone had Unix machines and Macs if they were lucky. 95 we had the first two day conference with 60 delegates who attended, 2016 we held our 25th anniversary in this building, we had a party upstairs, raise your hand if you went to that? That was a good night.

GOVIS continues to support people in local and central government to connect, share and learn about all the aspects of information, technology and business processes.

Again, in the beginning GOVIS was very technology focused. I remember ten years ago someone did a presentation about IPv6 it was called something being sexy, there was a joke in there about IP V sexy or something, I don't know. Crazy nerds, love it. GOVIS is run by volunteers, the traditional GOVIS people on the right, we have day jobs and that's Paddy and Christian and Finn and Chris McDowall. We also have -- I wrote these down so I wouldn't forget, Rochelle and Jacob who's away in, where did he go? Singapore, yeah. But we all work for regular normal adults jobs, but we do this because we love it, because having a conference and meeting all you fine people and helping government in this way is what we want to do

We also have lots of wonderful sponsors who make this thing possible, conferences are unbelievably expensive, the food bill is astounding. Eat all the food, we're paying whether you eat it or not, seriously. Am I right Christian? Eye watering. I'd like to thank our sponsors AWS, Catalyst IT and Catalyst cloud, thanks done Don, the OSS Group, IBM, he's probably out there, information leadership, this is the first time they've sponsored a GOVIS, thank you so much for coming around, and Middleware, thank you for coming back. I hope you find the day interesting and useful for you as sponsors as we do here. This is a unique opportunity to engage with the most important people in government.

Let's see is there anything else that I need to say? It's going to be a fantastic day. Hayley and Raynor from 12 conferences put together a wonderful -- they do all the staff that isn't content. The fact you have lanyards, the fact there's things that are printed out, that there's slides behind me is all Hayley and Raynor, we couldn't do this without them.

We also have -- there's a woman named Brenda Ratcliffe, the speakers are given the opportunity to do some speaker training with one of the nicest most enthusiastic people you'll ever meet to work on their presentations.

Unlike other conferences everybody who speaks at a GOVIS conference is a volunteer, they're not getting paid for their time, they've come because this is an opportunity to share their story and to network and share the successes and failures and Brenda does a great job of polishing up their speeches and working on them. It's one of the things I think GOVIS does that nobody else does did offer the service like Brenda does to potential speakers, so thanks to Brenda.

Finally there will be networking drinks at the end of the evening, some sort of drinks intervals at the end of it? Yes. And that's it from me. I will be hosting the Rangimarie 2 stream later on, you'll see me around anyway because I'm the president. At this point I'd like to hand over to Chris who's going to talk to us about the conference.

Thank you all for coming, I'm looking forward to hanging out with each and every one of you today. **[Applause]**

>>Chris McDowall: Great, thank you Mick. Kia ora koutou everyone, I'm Chris McDowall, I'm GOVIS Vice-President this year and my day job is working at MBIE in a team called data strategy and governance. GOVIS is much more fun. And today I think I'm probably the most over dressed GOVIS committee member but I'll let you all be the judge of that. We'll have to see when Rochelle gets here this afternoon whether I stand the test there.

So before I talk about what's coming up in the conference, I'm just going to quickly direct your attention to Slido. I think we might have a slide back one or two about Slido. So it's also on the back of your lanyard. If you just do a Google search for Slido, or whichever search engine you prefer, there should be a place where you can put in a number for the event code and so our event code is 1240080. So yeah, just search up Slido, put in that code, and then that will allow you to ask questions of the presenters, whether you're online or in person you'll be able to get your question in there. Unfortunately we're only do it for had this room so when we split into the session this afternoon, the people in that room will have to ask their questions in the time honoured fashion. For anything happening in here you can use Slido to put your questions through, and I think we've got an up voting feature, so if there's another question you think is really cool you can vote for than you one and the cream will rise to the top.

As well as that we've got some polls. So as I've been talking hopefully you've been getting into Slido and you've seen the first poll which asks a question. This is just to get a sense of who's in the room and who's online. What is your role or profession. Just self-identify yourself in there and we'll see what's coming through. So if we go to the Slido results please, looks like I'm not the only one doing data governance, maybe that's just because I put my answer in first it's promoted up like that. But great, we've got a range of people, cyber-security, information management, data governance, basically the same thing in my opinion, a Star Trek represented there, star fleet officer, got some sponsors, got some managers, musicians, excellent, how many have we got on here? We're up to 46. That's getting there. And a human. Great, we'd expect nothing less.

So if we could go back to the slides again please, keep your answers coming through there will be another poll very soon so stay tuned for that

Today as conference is all about digital resilience, and just to start off I'll ask the next question on the poll on Slido which is what does digital resilience mean to you? You've all signed up to come here and taken time out of your day, so hopefully you've all

got an idea of what the conference night be about by now, so just keen to see your thoughts on that. Just keep those coming and I'll keep talking about while you do.

So normally at the start of a GOVIS conference over the years we've had reasonably good success in cajoling a government Minister to come and open a conference. Unfortunately we were unsuccessful this year, our requests to Minister little's office went without a response, but to be fair we were probably a bit late in getting to them as well.

So we were scratching our heads trying to figure out who else could open the conference if not a government Minister. We finally came across somebody, they're extremely responsive and although they weren't able to join us near person they did give us a great opening statement for the conference. Which I will now read.

"Tēnā koutou katoa, welcome to this conference on digital resilience in the public service. Technology has changed our world and created new expectations from the people we serve. They want fast, easy, and convenient access to government services that are safe, secure and respectful of their privacy and rights. As public servants we have a duty to deliver for Aotearoa New Zealand, we have a duty to be resilient in the face of challenges and uncertainties. Resilience is not just about bouncing back from difficulties or set-backs, it is about adapting and thriving in a changing environment. It is about being prepared for the future and seizing the opportunities that technology brings.

To foster resilience we need to embrace digital transformation, we need to adopt new mind sets, skills and ways of working that enable us to deliver better outcomes for New Zealanders. We need to align our work to the strategy for a digital public service, which sets a direction for developing a modern public service that meets the needs of people in a digital age.

We also need to support each other as tech knowledge information and data professionals. We need to collaborate, learn, improve, and take care of our own well-being and balance. This conference is a great opportunity for us to do that. I hope you will find it valuable and enjoyable, thank you for your attention, kia ora koutou katoa. "

So I'm sure you'll agree that sounded pretty good and maybe something that a Minister would have said at an event like this. But you can probably guess what that was. Yeah, so that wasn't a human at all, that was a large language model. I actually used Bing chat just for a change, but it's actually based on chat G BT for anyway. It only took me four prompts to get that response. The first prompt was just asking about resilience in the public service generally, that was quite good. Then I asked about digital resilience, that managed to get quite specific. Then I asked for it to give that to me again, but in the style

of a government Minister opening a conference, and then it was quite long so I asked it to cut it down. I asked it to cut it the down to 200 words and it was very responsive there. So we'll have to review our tradition of inviting government ministers to conferences. Maybe we've come across a better solution, I'm not sure. At the end of the day I guess it goes to show it's not what you say it's also who's saying it and the process which you've been through to kind of get that answer.

Yeah, I could have gone further but I didn't. We could have had some sort of avatar saying those words on the screen but I thought I better not go there. So this technology is obviously a big deal. AI's become much more capable and much more available just in the last 6 or eight months. I think my brother was the first person I met who'd made good use of it. He wrote all his Christmas cards using chat G BT and I don't think anyone notice until he told us afterwards.

But there are challenges as well, as we'll know, so Bing chat for example had some problems with its persona going a bit crazy and off the rails. Then more broadly there's also the question of what happens to all the prompt information that we're feeding into the tools, it can be used to retrain the modelled and regurgitate today someone else. Yes, it probably can. So as we've probably heard in the us in this has led to some government departments, including MBIE where I work, to block chat GPT and the office of the Privacy Commissioner in New Zealand has also issued some pretty specific guidance.

But on the other hand of course we want to be taking advantage of all of this revolutionary technology and learning how to apply it to our work. So we'll go back to Slido. This is what we had here and what digital resilience means to you by the way. Future-proofing, security risk and assurance, preparedness, there's some great answers there. You've been able to see that on your phones as well. Herding cats.

But now we'll go to a new poll and, let's see, this is a bit of a straw poll to understand your own familiarity with chat GPT or similar tools. Have you used it yet? No, yes, but only for fun, just in my personal capacity to try it out and then yes, I'm actually using it at work as a productivity tool. I put myself in the second category I think. Yeah interesting, sort of a fifth, just under a fifth of us using it as a productivity tool. We might have to ask this question again next year and see if it's increased.

The next question is, does your organisation actually let you use chat GPT or similar AI tools at work. If you work at MBIE like me you'll be a no, I think DIA, the GC D O are encouraging staff to experiment with it and try it, I could be wrong0 maybe I'm not

sure, maybe you haven't tried. Over half of us we're not supposed to be using it at work or on work devices, we'll have to see how that shifts as well

Back to the slides, I'll just quickly wrap this up. I need to finish by 9.30. Just going back to the theme of digital resilience, we wanted to think about digital resilience at three levels, over on the left there. National resilience, geopolitical considerations, then down to institutional resilience, what it means for us as public servants working in large organisations, and then down at the personal level, and Bing chat actually managed to nail most of those.

We also wanted to call-out three topics which are relevant, cyber-security seems to always -- there's always something in the news about a new breach or a new hack or something like that. It just keeps on increasing I think in scale. We also wanted to call-out resilience and sovereignty in the cloud, we've got a panel coming up about that later this morning, with big cloud computing companies and coming to New Zealand to build data centres, what does that mean for New Zealand, what do we need to be anything with, what's the opportunity. Finally incident response. So we've had the Auckland anniversary floods, cyclone Gabrielle, we're going to continue to have disasters that need responding to, how can we be ready for that, be better prepared and more effective in our response.

We also need to think about the outcomes of digital resilience, I've put those over on the right-hand side. The first one there is deliver better outcomes for people in Aotearoa New Zealand, this is just pulled off the Public Service Commission website, what's the purpose of the public service, that's us. We need to be honouring Te Tiriti and respecting human rights. At last year's conference we were lucky to have Paul Hunt the Chief Human Rights Commissioner come and speak to us a bit more about human rights. Then finally we need to be operating within environmental limits and being good kaitiaki of te taiao. So the we've got carbon emissions to watch, there's biodiversity and all sorts of other environmental measures we need to be operating in as well

Then finally in the last six months ago once the conference theme had been decided AI has come on the scene in a new way, bringing opportunities and risks and there's plenty for all of us to learn.

So today you've all got opportunity to hear some amazing presentations and have conversations about all of these topics. I hope you have a great time and then to bring it back to our motto at GOVIS, treat it as a chance to connect, share and learn. Thank you.
[Applause]

9:30 - 10:15 am: Building Cyber Resilience: 5 Things you can do Today

- **Michael Jagusch**

>>Paddy Power: Thanks Chris. That was a great way to kick off the conference I thought. So I'm Paddy Power, I'm on the GOVIS committee, I'm senior manager at Stats NZ in my day job. I'll be your chair for this morning's session in here. I'm here to introduce our first speaker who is Michael J, I knew I was going to stumble over that. Mike is the mission enablement at the national cyber-security centre. Sounds like this guy works for NASA. He has several roles within the national cyber-security centre and a broad experience within cyber-security. He's worked in customer engagement, providing organisations with security advice and guidance, both at a practitioner and a governance level.

Previously he's been involved in the more hands on aspects of cyber-security in his role managing the systems engineering team who design, build, maintain and evolve NCSC cyber-security capabilities. In his current role he's focused on delivering strategic outcomes by leveraging the expertise by the entire NCSC. Mike's team provides communications, policy, stakeholder engagement and business support. And Mike is going to be talking about building cyber resilience, five things you can do today. Welcome to the stage Mike.

>>Michael Jagusch: Tēnā koutou, tēnā koutou, tēnā tātou katoa, (pepeha). Good morning and thanks for the opportunity to talk here today. I must admit sitting there listening to the introductions, this is really intrigued me up on screen, I assume, is that an AI picking up, no it's someone typing? Wow, okay, good, it's good that humans are still more efficient than an AI, I very much liked how when there was an applaud, the applaud came up and I thought if it was an AI if you tell a joke your goal must really get to have the AI pick up laughter, and if you didn't it would be a bit unfortunate.

So as per the introduction in my 10 or so years at the NCSC I've had a lot of exposure to a lot of different people tackling -- I guess what I would call different parts of a complex cyber-security challenge, from boards all the way down to hands on IT security people. And what I've found that a lot of people almost get a little bit overwhelmed by what they perceive to be quite a complex area and they may be don't know where to start. And the people that I see do really well, are people who would break down a complex topics, they're able to break it down tackle it bit by bit and able to communicate well about what they're doing. So today I want to focus in on giving you all five things I think that you could focus on and give you some tips around how we at the NCSC talk about and

think about cyber-security and maybe these are some helpful things you can take back to your organisations.

Before we get there though I'll talk a little bit about the role of the national cyber-security centre, a little bit of the overview of the threat scape in New Zealand and then I'll get into those five things that you can focus on.

So first of all I'll start with who we are. So we are the national cyber-security centre and we are part of the Government communication security bureau. We take advantage of our unique position as an intelligence agency to fuel our cyber-security mission. We're focused primarily on the cyber resilience of nationally significant organisations. Those are organisation NCSC the public and private sector on who's continued operation New Zealand's security well-being and economy depends.

We're also focused on what we call national level harms and often this involves focusing in on a state sponsored actor, that is a malicious cyber actor who is being resourced or sponsored by a foreign government. But over time this is changing and evolving to encompass threats or vulnerabilities that could present major challenges to New Zealand's economic and social well-being that often aren't coming from a state actor anymore

Cyber-security is a really broad topic with multiple dimensions and is important to all New Zealanders. When I talk about cyber-security I'm primarily talking about security at the organisational level as opposed to keeping your own Facebook or LinkedIn or Twitter secure.

So with all of that in mind we have our three overarching strategic objectives, defend national security, raise cyber resilience and facilitate digital transformation

Now we work towards these objectives through providing a range of cyber-security functions. These include services focussed on the protection of classified information. We have a regulatory roll over a range of sectors, and then we provide preventative advice, threat detection and disruption services to our customers.

When all else fails we also have an incident response capability where we help victims respond to severe incidents. We group our services under these four areas that you can see on screen, detect, disrupt, advise and deter. Firstly we detect indications of malicious activity, vulnerabilities or weaknesses across New Zealand. We do this through some technical capabilities that we have, but we also do this through extensive customer relationships just getting out and about and hearing about where organisations are struggling. We then disrupt these threats from harming our customers' environments. This

can range from deploying staff to work alongside a victim of an incident, or it could be about releasing an advisory on our website about a particular threat.

We also have a technological disruption capability called malware free networks. Through all of this detection and disruption activity we develop a broad understanding of the New Zealand landscape including the threat scape and where organisations are struggling. We use this to create advice that helps our customers to focus their security efforts.

Now as a result of all of our efforts, our goal is that we are deterring our adverse Rees because we are raising the cost of conducting malicious cyber activity in New Zealand. We're making it harder for adverse Rees, we're taking away the easy wins that they may have.

We represent this as a circle because we're very conscious as we raise -- as we work with others to raise cyber resilience throughout the country, our adversaries or the bad guys are also constantly evolving the techniques they're using and using new tools and so we then need to detect these, disrupt these, create advice and the cycle goes on

Also the technologies or the IT environments our customers are using are constantly changing, we've talked a bit about chat GPT already today, so we need to make sure our service offering keeps pace with the technologies people are using in their organisations.

So our service offering here represents a multi layered approach required to tackle cyber-security challenges. We really encourage organisations to do the same. That's something that I'll talk about later on.

Now we don't do all of this work just for fun. We do this work because there are threats or incidents that occur in New Zealand.

So we deal with about an incident a day, ends up being about 350 a year. It goes up and down around there, but it's relatively consistent over time, around that one incident a day. Now it's important here to remember, because we have this focus on nationally significant organisations or national level harm, this is likely a very small proportion of the amount of incidents that happen in New Zealand. I know when you start to talk about incidents affecting individuals, for example, you get up easily into the 60, 50,000 per year I believe are the numbers that CERT New Zealand report.

So I think one of the most interesting things in terms of these incidents is that around a third of the incidents we deal with they are linked to state sponsored activity. And the scale of state sponsored activity against Aotearoa makes it challenging to identify, track

and record, because these actors are constantly evolving their techniques and tactics to he is scale detection for as long as possible

These actors are also less likely to cause immediate disruption to a network or cause something that's obvious or public. They are more likely to conduct activity to support espionage or their economic development. And this can involve the theft of information and intellectual property.

Now organisations who report incidents to us do so in confidence, so I can't share all of the details of these incidents but there are a couple of key themes I want to pull out.

First of all we see that vulnerabilities scanning and gaining access to an internet facing device remain the most commonly seen cause of incidents. This continues a trend where sophisticated actors look to take advantage of known vulnerabilities. So we continue to see an increase in the speed and scale of mass exploitation of known vulnerabilities. What this means when a hardware or software provider goes public that there's a security flaw within their products, we see malicious actors effectively scan the internet to find those devices.

They take advantage of these flaws, they establish foot holds and then they selectively return to certain targets to conduct further activity.

A key point I want to make here is that all of the incidents that we deal with are preventable and there's normally information available for people about how to prevent them. Adversaries are also taking advantage of weaknesses within supply chains or thrust relationships. The two most severe incidents out of those 350 that we dealt with were actually connected, analysis revealed that after the malicious cyber actor compromised the first organisation, they used its access to target the second organisation by exploiting a trusted relationship that the organisations had between each other.

So Aotearoa's security interests are being challenged by the international rise of strategic competition. States are more readily pursuing their strategic objectives in ways that undermine the rules-based order that we have relied on. These geostrategic shifts have presented opportunities for state and non-state actors to use malicious cyber activity to seek persistent, strategic access to networks.

It's really clear that even in New Zealand, our domestic threat scape evolves alongside geopolitical trends. The primary example we have of this most recently is that this year we actually had a slightly reduced amount of incidents around 50 less than we normally would in a year, and our assessment is that that was actually because of Russia's invasion of Ukraine, so even though that is very far away from us, we know that Russia and

other Eastern European actors feature significantly in the global cyber threats landscape. So our assessment with the Russian innovation of Ukraine, these actors from that region have been more focussed elsewhere rather than conducting activity that would previously have had an impact on New Zealand.

These heightened geostrategic tensions have impacted the institutions, rules and norms that we have relied on and it's likely that as geopolitical competition continues to rise, there will be ongoing implications for our networks in New Zealand should malicious actors attempt to leverage these capabilities for strategic advantage.

Now to give you some quick insight into what these state sponsored actors look like and the type of ac shift they do I'll talk about two advisories that we recently released

The first one we joined our partners in releasing advisory with activity associated with the People's Republic of China. This activity had been observed affecting critical infrastructure throughout the globe. These actors used tactics techniques and procedures that we call living off the land, so that is about using built in systems within IT systems, built in functionality within IT systems, and they do this to avoid detection because it looks like normal activity.

Then earlier in May along with our international partners again, we released an advisory about malware used by Russia's federal security service. That they use for long-term intelligence collection.

The most interesting take away for me out of both of these reports, as though in both the activity is described as highly complex, technically sophisticated and extremely significant resourcing behind it, the mitigations are incredibly basic.

So in terms of the sophistication, a quote from the advisory around the Snake malware "we consider snake to be the most sophisticated cyber he is pi imagine tool in the FSB's arsenal, the sophistication of Snake stems from three principal areas. First Snake employs means to achieve a rare level of stealth. Second, Snake's internal technical architecture allows for easy incorporation of new or replacement components. And lastly Snake demonstrates careful software engineering, design and implementation with the implant containing surprisingly few bugs given its complexity."

So quite a stark picture that paragraph paints. Then if you get to the mitigations to how to prevent the Snake malware from having on impact on your network, the top four mitigations are change default passwords, require minimum password strength, require unique credentials and separate user and privileged access accounts. These are mitigations that have been well-known and around for a long time and are relatively simple. These are

the mitigations that would prevent a state sponsored activity from having an impact on your network. To me this is a clear example reinforcing even the most sophisticated actors primarily look to take advantage of well-known flaws

Another key trend we observe year on year is the blurring of lines between state and non-state actors or criminally or financially motivated actors. We have we're increasingly observing these financially motivated or criminal groups using capabilities that until recently were only within the domain of state sponsored actors.

This growth in sophistication is particularly concerning because these actors are more likely to cause disruption to a network, and careless about the international politics associated with conducting this type of activity.

The increasing availability of cyber capabilities reduces technical barriers to entry, enabling any group with purchasing power to conduct these types of operations.

One of the most commonly used techniques by these criminal actors is ransomware. Ransomware activity targeting New Zealand is increasing over time. Some of the most common ransomware variants we see are highly likely marketed by groups that operate ransomware as a service. This is a business model that involves selling or renting ransomware to actors who independently compromise networks and deploy the ransomware.

These groups can be typically -- can be sophisticated and well practised and similarly that he can adapt their techniques over time based on what makes the most money for them.

In recent years ransomware operators have taken to finding and destroying or encrypting data and back-ups and then copying large amounts of data so they can conduct a double extortion where they ask you first of all to pay to have your data or your systems unencrypted, and then they ask you again to pay so they won't publish that information online.

We've also seen ransomware actors actively monitor the media to understand the level of impact they're having on your network and using this as leverage to increase their ransomware demands. Our analysis shows one of the top two sectors impacted by ransomware in New Zealand are healthcare and the manufacturing sector.

So it's a realistic possibility that these cyber criminals target these sectors, particularly the health sector, because they recognise that health organisations are more likely to pay a ransom or extortion fee because down time to IT will become a threat to life.

Early this year cabinet confirms that government agencies should not pay cyber ransom, there's a lot of legal reasons for that but from a security perspective it's also important to remember that paying a ransom doesn't actually guarantee that you'll get your systems or data back, it equally might put a target on your back because someone knows you paid last time you may pay again. Instead like other types of malicious activity ransomware activity is preventable. On screen is a great visual from our colleagues at CERT New Zealand which demonstrate there are multiple opportunities where effective control could stop a ransomware event. Each octagon up there is one of CERT's top 10 critical controls, they have lots of information available online on implementing this control. What the image shows is that a lot needs to happen before the impact can be felt on your organisation.

So if the mitigations are well-known and somewhat obvious, why are these attacks successful? I think a lot of that has to do with the fact that people may not know where to start or where to focus their efforts.

So to help with this we've recently released the New Zealand cyber-security framework and we've had some really good input from people across New Zealand to develop this framework and we've release what had we call a beta version, so still open for some feedback

Our goal here is really to demonstrate what good cyber-security looks like for other organisations and we're making this framework publicly available, it's on our website if it suits your organisation.

The framework sets out how we think, talk about and organise cyber-security efforts. And its five functions on screen represent the breadth of work needed to secure an organisation. People familiar with the NIST cyber-security framework may see some similarities and we've based it heavily on NIST, but we've adapted it for our context here in New Zealand. The main point of difference here is that we've chosen to place greater emphasis on security governance and culture by separating it out as its own function.

As I said earlier we encourage organisations to make sure they have a well-rounded approach to cyber-security and we view this framework as a really helpful way for organisations to assess their current cyber-security priorities and see if they are focusing in on these different functions

So the framework is composed of two parts, the interrelated concurrent cyber-security functions you see on convenient and then for each of those functions we have five security objectives. This is probably the other biggest change we've made to

NIST, while NIST has over 22 categories and 100 subcategories, we have 25 things for people to think about to make it a little bit easier and also recognising a lot of organisations are already using existing frameworks, we feel this will make it a little bit more approachable for them

So we're really hoping this framework helps senior leaders and executives understand cyber-security and what their organisations are doing. We don't expect decision-makers to understand all of the technical detail of your cyber-security road map, but they should be making sure that their organisations are taking a well-rounded approach to cyber-security, and investing appropriately across the different functions and not over investing in certain areas. I guess the key thing we see is often organisations focus a lot in on the technology solutions or the detection, and what we're really encouraging people to think about is more broadly, think about cyber-security more broadly

So I'll use this framework to give you the five things to focus on today, one for each of the functions. So firstly, guide and govern. So this is about cyber-security being promoted through governance efforts and I by providing guidance to your people. The objectives here are to embed security principles and practises across your organisation so that cyber-security supports the organisation's outcomes.

The second objective is to make sure that people don't have to be security experts to use your systems. The third we encourage you to prioritise your security investments to focus on real threats to your organisation and make sure that investment is continuously focusing on improving your security posture.

You should also make sure that you receive assurance internally and externally that your security efforts are effective, robust and adaptable

The key thing I'm encouraging you to focus on here is security awareness training. Cyber attackers often rely on human behaviour such as clicking links or downloading and opening files to give them valid credentials or access to a network or system. Our partners at CERT New Zealand find over 82% of the incidents that they deal with have a human element.

The first thing I would check if I was survivor to make sure that for your security awareness training you're doing more than just a one-off video or module as part of an induction programme. Security awareness should be continual as cyber-security messages should form part of your regular corporate communications, not every week, maybe once a quarter is a good target

Another key thing to keep in mind is establishing a culture where you don't blame victims. You want people to report incidents to you, you want people to report near miss stakes, because it gives you a sense of what's actually happening.

Then the second area identify and understand. This is about knowing which cyber-security activities you are responsible for and where across your IT environment you are applying them.

Your objectives here are that you should understand your organisation's appetite for balancing risks against opportunities. You should make sure you have an understanding of your key information assets, you should understand how your organisation and assets could be targeted. What's your threaten environment you're working with? You should understand any Māori data you Holland ensure you are clear about treaty partner security expectations. And you should make sure you understand how your supply chain or your IT providers and relationships affect your security posture

So the one thing I'm encouraging you to do today is to make sure you're using the same tools, techniques and languages to manage cyber-security risk as you are other risks in your organisation. In most organisations risk management frameworks are welled and understood and you probably have them existing for things like health and safety for example

Cyber-security risk should align to these frameworks, because it gives consistency in risk management and it also frames cyber-security in a way that is familiar for the organisation and the decision-makers.

This can be as simple as making sure your IT security teams are using the same Excel spreadsheet. This approach here using your existing risk management frameworks can also help you make a well informed and nuanced decision about the use of something like chat GPT which we've already spoken about.

Third prevent and protect. This is about focusing on reducing actual risk and focusing on incremental improvement, rather than thinking that you will achieve perfect security tomorrow. Your objectives here are building security and privacy into systems by default, making sure you separate systems so you can choose who is given access to what, based on their role within the organisation. You need to keep your systems up-to-date, applying the latest patches and addressing new vulnerabilities as they are disclosed. You need to think about using modern security tools like multi-factor authentication and detection tools, and you need to identify and protect any Māori data in line with treaty partner's expectations

The one thing I'm encouraging you to think about today is the use of multi-factor authentication. With a particular focus on systems that hold sensitive data are used by administrator users or are accessible over the internet. These should be prioritised for multi-factor authentication

There are various methods for implementing multi-factor authentication, I encourage you to find one that works well with your business model. Unfortunately some multi-factor authentications methods are also vulnerable to attacks, so stay away from something like text verification and move towards something like a physical token. You could also consider implementing multi-factor authentication for a critical business process, for example paying a large amount of money to an external request. You could have a process where these staff need to follow or request need to be given in a separate communication channel before they are made.

Detect and contain. This is about being realistic that threats or incidents may occur in your organisation and you need to be able to contain them. Security monitoring is a necessary component of knowing when normal activity is occurring. You need to make sure that you are monitoring what is actually happening on your systems, and can tell when things are not operating normally. You need to continuously review and check that your security controls are effective, you need to minimise and monitor the interaction between your different IT systems, and you need to make sure you control the ways in which your information moves between systems.

You should also make sure that you have a way to isolate systems when needed.

The one thing I'm encouraging you to do here and yes this is 100% a shameless plug for a service that we offer, I'm asking you to check whether or not you receive the national cyber-security centre's mall way free network service and if not talk to your IT provider about whether or not you could access it.

Now malware free networks is a cyber threat disruption service we deliver in partnership with private sector in New Zealand. Based on our visibility of threats we generate indicators of compromise based on what we know of indicators of compromise that give you a clue if bad things are happening, and we disseminate this to our partner organisations and then our partner organisations then use this threat intelligence to detect and disrupt cyber threats to their customers. We've disrupted hundreds of thousands of malicious events this year alone.

One of the really interesting findings through operating this capability is that although we use international sources to help develop our threat intelligence, the vast

majority of events that we disrupt come from domestically sourced indicators. This suggests that there is a unique New Zealand threat landscape.

Finally, respond and recover. So this is about prioritising your security incident response to get critical services back to normal operation as fast as possible. The objectives here are to develop response plan that focus on likely events, not doom's day scenarios. Make sure those plans are flex will and can adapt as you gather more information. You should understand where you can get help from and the level of service that you can expect from your providers before an incident happens. You need to know your critical systems and how they contribute to business objectives so that you can prioritise what you need to restore first in an incident. And you should also make sure you're practising your response plans to improve them and have confidence they will work

The one thing I'm encouraging you today is to check whether or not you have an incident response plan. Secondly check that it is up-to-date. The reason for this is cyber incidents are really stressful situations and often for you and your teams if you're involved, it may be the first time you're ever involved in a cyber-security incident. Hopefully the last as well. You'll need to make quite difficult decisions without perfect information. While that happens in a lot of other incident response activities, natural disasters and others, the thing to remember is there will be a bad person who's actively trying to make this harder for you as well. So there'll be some really complex decisions to make where you balance up security versus getting services back up and running. How do we know that we are restoring to a known good state and things like that

So without being too cliché a lot of this uncertainty and stress can be managed with a plan that is regularly tested. It really helps to reduce some of this complexity and stressful situation and if anything, although you wouldn't have exercised the exact scenario you are in, I think as humans we really enjoy the fact that we have a piece of paper to fall back to that has clearly articulated the steps that we're going to take, and a plan is also really useful for communications because you can really clearly communicate where you are in an incident response process, and when you're at an early stage, for example, people may be expecting you to have a lot more information than you do, and when you have a plan you can refer them back to that earlier on in your plan.

A plan should describe who is responsible for making these types of decisions. I really recommend you sort that out before an incident. If you're clear on who has responsibility for decisions, it makes that actual decision a lot easier, rather than also trying to figure that part out during an incident.

So check your plan is up-to-date since your last organisational restructure or re-alignment, often just the role titles will have changed, people may have been mentioned and moved on, so that's a really good first step, just making sure the roles and responsibilities are still relevant for how your organisation is structured

Three things that I've seen organisations do well during incident response, firstly and we've already talked this a little bit, people who are able to describe choices in terms of the risk choices in a way that aligns with your organisational risk management processes, once again it just brings that familiarity to the decisions.

People who are able to use scenario generations, they're able to tell a good story about how things could play out, and they're probably moving beyond just the technical or the IT aspects, they're starting to talk about impact on your business, impact on your customers, and where this incident could be heading.

And thirdly, people who know who their trusted advisors are internally, but also externally. If you're relying on vendors and you're paying vendors for incident response services, know what you're paying for ahead of time rather than trying to litigate that during an incident

So as I said at the start, cyber-security is an important topic for all New Zealanders, and I think one of the most interesting things about cyber-security and the thing that keeps me working in this area is it's probably the only area of national security where literally everyone matters, especially if you're working in the public sector, we all have a role to play in protecting the security of our information and therefore potentially the security of our country

We recognise at NCSC we can't do this all on our own, we continue to find ways to scale our efforts to collaboration and partnerships and talking at conferences like this is a really good way to share our perspective and also hear a little bit more about what other people are struggling with so we can make sure our advice and guidance is keeping pace with what people are actually dealing with in their organisation.

I really hope that my talk has highlighted that although this topic can be complex, we are operating in a constantly evolving threat scape and the technology we're using is constantly changing as well. The reality is that taking small steps can make a huge difference to your organisation and therefore the country's overall cyber resilience.

Almost everything I've talked about today is available on our website and I have my contact details coming up shortly if people are interested in more. So go away, think about these five things. If you've already done these five things, find another five things to figure

out, and keep going like that. That's really how I would approach it. You won't become cyber secure overnight. In fact we don't often use the term cyber secure anymore, that's why we use more towards things like cyber resilience because the reality is there's probably not an end state it's about consistently moving and becoming more and more resilient.
I look forward to answering some questions, we'll be around for the morning tea break to continue conversations. And as I said, interesting area of national security because we truly all are in this together, he waka eke noa. Nō reira tēnā koutou, tēnā koutou, tēnā koutou katoa.

Q&A - Building Cyber Resilience

>>Paddy Power: Thanks Mike. I thought that was great really practical advice there. So we've got some questions on Slido. If you're not on Slido have a look. You can vote questions up or -- I don't think you can vote them down, but people -- you might be more interested in other people's questions, or you might want to put in some of your own. First one we've got here is do you think cyber-security is getting enough attention from government organisations, especially executive leadership teams? What do you wish they knew?

>>Michael Jagusch: I think for me my frame of reference when I got this -- similar questions to this, when I started doing this around ten years ago, we'd go and speak to a board, we would be very much starting in what I would call cyber-security 101, it's a thing, you are need to think about, threat, threat, threat, some scary stories about some things, and then we'd leave and I'd say we were definitely realising we were giving this information to people for the first time. Now if I think about when we go to a board and talk, they are asking us specific questions around I have -- my teams tell me we should do this or this, which one is better.

I guess my assumption from learning that is that people have moved a long way, people know the basics and now they have a plan in place and they're really trying to get some detailed information about what to do next. So I think it is definitely getting better.

I think the thing I wish that all executives knew is probably a little bit about what I've talked about today. I think probably one area where cyber-security professionals struggle is almost the story telling or the narrative around cyber-security, so I do worry that some boards get presented a risk register with heaps of red dots that says everything's impossible and all our systems are old and we don't have enough people. I do worry that there's a little bit of on cyber-security professionals for us to improve our ability to tell a

story around yes, there are some challenges out there for us, but we've chosen these things to focus on because that will make the most improvement for us.

So I'd encourage the executives if they're not getting the right information that they need, we have a lot of information available for our guidance around the top sort of questions that we would encourage executives to ask their IT security seems so they get the information they need.

>>Paddy Power: Thanks Mike. I might put these two together if that's already. I'm not sure how many Mike is actually going to be able to say about these questions. But are we living in an era of digital cold war and foreign state actors test our national and institutional systems for vulnerabilities. Presumably we do the same of other sovereign nations? I think I can probably -- if we do you're not going to tell us that.

>>Michael Jagusch: That's all right. I'd say on the second one, it's probably important to remember that cyber-security or malicious cyber activity would be part of an organisation's overall foreign policy approach, so when we talk about actors who conduct these types of malicious activity, that probably aligns better with how they view the world, so if you think I've talked about advisories about Russia and PRC, we also so Russia invade a country recently. So malicious cyber activity is part of ow an organisation promotes itself internationally. So you'd really need to think about whether New Zealand's place in the world and how that sort of activity would line up with how New Zealand plays as a international player and how that lines up with our overall approach to foreign policy.

Are we living in an era of digital cold war? Interesting question. There is quite a lot happening in the moment around the setting of international standards. So the internet effectively is governed, the protocols that guide the internet are governed by international bodies. I think a really interesting thing for us to see play out over the next year, the coming years, is whether those, the kind of existing standards that we have for the internet remain, or whether certain states look to promote their own interests and how the internet is governed. So I think it's an interesting space to watch, and probably would line up with that statement around how we know that New Zealand and our role in the international rules based order is potentially being challenged currently, will we see more of that play out in the way the internet governed.

>>Paddy Power: We've probably only got room for 3 or 4 more questions, there's lots of questions here, obviously lots of interest in what you've been saying Mike. Security and privacy are often seen as the big black hands that stymie transformation in an organisation, I've definitely heard those kinds of conversations going on. How do you avoid that?

>>Michael Jagusch: So that's about -- the way to avoid that is once again I think it's to put security -- I'll talk about security more than privacy, to put it alongside how your organisation makes decisions on other things. So to use an example, I'll use social media as an example. So people will be aware lots of media interest around TikTok and hey we should been a TikTok. But actually what we encourage organisations to do is to run that through a pretty standard risk management process, of which the first step should be what is the business need for this, so if you think about social media application like TikTok there, is likely some business needs to use TikTok especially for government agencies to reach audiences they might not otherwise be able to reach.

So once you've established a business need, then you can work through the security or privacy implications and the security implications shouldn't always be -- shouldn't Trump the objective. So if I think about social media for example, if there's a business need to use social media, but your organisation -- to use TikTok but you're concerned about some of the threats or risks associated with that, that doesn't mean no, it means you should look at some compensating controls around it. For example, you could only have TikTok allowed on certain devices, you could provide extra training for the staff who need to use that, you can make sure you monitor those devices for additional threats. So I think that's the way that you need to approach these things. First of all does our business need it, and if yes, it's more about how do we make it secure as opposed to the business need and the security being traded off against one or another, because security should help our organisation, security shouldn't stop our organisation.

Once again I'd think about how you make decisions on other risks, businesses make decisions on risks every day. How are you making those decisions, and then how can you apply that to security.

>>Paddy Power: I think we'll take this question which I think is a slightly different angle here. How do you maintain resilience at the national cyber-security centre itself given you're dealing with so many threats. You guys must be dealing with --

>>Michael Jagusch: One a day.

>>Paddy Power: Several a day. How do you keep your mojo with all that going on?

>>Michael Jagusch: I think to be honest we're very lucky that people are quite interested in this space, our staff are really passionate about it, it's a really -- it's quite a fun place to work I must admit. You might be out doing things like this today. We may have some other staff working alongside a victim in incident response, we may have staff on a conference call with the NSA about latest threats, so there's quite a lot of different elements that I think

keep us all interested. And I think it's also becoming just more and more clear how intertwined cyber-security is becoming with all of the other objectives that people have, so we're becoming a really -- cyber-security is becoming a really important part of all businesses and all daily life.

I think that interest keeps us going. I think other than that there's some more practical things about keeping our mojo, so we categorise incidents so that we make sure we are providing a proportionate response to an incident based on the threat and impact, we look to establish good people rosters when an incident kicks off, so that people aren't working 24/7, we make sure that we get some food delivered if we're working overnight and things like that

So I think it's relatively standard stuff that I'm sure most organisations are facing. And then I think there's a wider resilience thing around just making sure we're able to recruit staff interesting in this area and then retain them. And there is a pretty competitive private sector environment that we're competing for skills with. So that's why we're lucky to have that national security focus which can keep people motivated, even if they may be able to get more money elsewhere working for a private sector. But drawing them back to that overall mission and what we're here to achieve seems to help us out

>>**Paddy Power**: I think we'll have to wrap it up there because we're heading for morning tea. Thank you very much Mike. As I said I thought that was really practical and engaging presentation. We've got a little gift here from GOVIS. So thank you for that. If we can all thank Mike in the usual way. **[Applause]**

Now we're going to go to morning tea and which is out in the, what do we call that area? The place where the food is. So we have a dark chocolate cherry brownie, tomato goat cheese pastry and the tea and coffee. We have some sponsors in that space, encourage you to go and chat to the sponsors, we can't do it without them. We'll see you back at 10.45.

10:15 - 10:45 am: Morning Tea

10:45 - 11:25 am: Security and Sovereignty in the Cloud

- **Dr. Te Taka Keegan, Louisa Joblin, Don Christie**
- **Chair: Phil Pennington**

>>Paddy Power: Just to get us settled in, can we have the Slido up on the screen? We've got a couple of polls. So would you rather have weekend away with pirates? Or ninjas, right now? 100% pirates at the moment. 60% pirate in this audience. I think we have another poll now. Would you rather give up air-conditioning and heating for the rest of your life or give up access to the internet for the rest of your life? I think I'd choose air-conditioning. I don't think I can cope without the internet. 32 votes so far and that's very close.

Okay, I think we can go off Slido now. I'm just going to introduce Phil Pennington who is chairing this panel. I don't know if you went to the GOVIS conference last year, we had a panel which was also chaired by Phil and I think he did a great job of chairing the panel and I think the great thing about Phil is he's not a public servant, he wasn't polite, he really asked some tough questions, and people really enjoyed that, we got a really positive feedback. So we've invited Phil back again this year to chair another panel and I'll hand over to you.

>>Phil Pennington: Thanks Paddy, ko Phil Pennington ahau, (te reo Māori). I'm Phil Pennington, I'm a reporter with RNZ, I live in the Hutt and my favourite place and my dog's favourite place is Te Awa Kairangi, the Hutt river. Thanks for having me back, thanks for the kind words Paddy. If I have had any interactions with people on the phone, I apologise now, I hope you'll give me a break, but thanks for having me and thanks for having us, just want to introduce the panel.

What we're talking about this morning is about the cloud and cloud fist and sovereignty and security, so those four things keep them in your mind. We'll introduce the panel, just give a little bit of an intro then I'll have some questions for them, curly questions, then we'll have a bit of time when we can get questions from abroad and from the floor and we'll see how we go.

Our panellists today are Dr Te Taka Keegan who is a veteran computer scientist at Waikato University, he's been surveying Māori data and its interactions including with the state for a long, long time, including the discussions with open access. Welcome Dr Te Taka.

And our other panellist is Lou Joblin, Lou, welcome, she is a senior associate at Duncan Cotterill. She's working in the field of privacy and data protection, she does a lot of advice for individuals and for agencies. And on the far end Don Christie, ex-Zambia and what waka was it you said you came over on? Mawingo, Swahili for little cloud, came from Zambia. Don Christie is the Managing Director at Catalyst IT, that runs Catalyst

Cloud which is the only locally all of government accredited cloud provider alongside some of the big boys in tech.

There's a dilemma we face, it's illustrated by a couple of New York Times stories. There was the one tine statement put out last week or two weeks ago by AI luminaries like the head of Open AI, the guy who runs it for Google, and there's one line basically said AI is now an existential threat and should be addressed in the same vein as climate change and nuclear weapons, that's on the one hand. At the same time in the New York Times there was a story about a lawyer in Nebraska, a senior guy who put got all these legal briefs in chat GPT and chucked them into the court in support of his case only to find out of course they were completely fiction lied when they asked him what due diligence did you do on these legal briefs he said he asked whether they were correct and they said who did you ask, he said I asked chat GPT.

What the New York Times podcast hard fork, that's where you start an IT project, you mess it up completely and then you have to throw everything away and go down a hard fork. Anyway it's called hard fork. They said what this illustrates is you've got a dilemma which is where the IT, the tech is not good enough and you get a bad result, that's the lawyer, or in the long-term it's too good and you get a bad result, existential threat. You can also see this with facial recognition, the short-term problem of not good enough is that it's biased and people get locked who didn't do anything, so then the impetus is to do it better and better, but then you get a long-term threat which is you get a China situation, mass, very effective state surveillance.

So in solving the short-term threat with the IT, you run a risk of creating a long-term threat with. The cloud I'd like to just hold your attention on that tension, because you work in government, you work with a cloud first policy, and it can be argued that you have a short-term problem which is masses of data, storage and processing, and what to do with and that's your security I'd argue. Then the long-term problem is as you try to solve that short-term problem of the cloud with security you introduce the long term problem of sovereignty which is what we're talking about today

So I hope that made sense. It made sense to me anyway this morning, but I got up pretty early and I missed my train and it was very, very cold and the head wasn't working very well. Then this morning I was reporting actually on the radio on critical national infrastructure, so that's the other thing to bear in mind, critical national infrastructure, what they're doing in the government now, there's a bill, consultation, you all work in this field and the cloud is critical national infrastructure, what was interesting is the papers drawing

on for the radio is it says in them, the advice from the officials is that, if I can find the quote, there is no -- it says, "the risks including national security risks facing critical infrastructure are increasing at the same time as our regulatory system is being out paced by technological change. For example cloud service providers data service storage providers and forthcoming technologies to support smart cities and internet of things all sit outside New Zealand's existing regulatory frameworks. They are not subject to regulation around their resilience at all", that's talking about the cloud.

Our first question, I think Lou we'll start with you. So Lou, in terms of the cloud and we're talking about the cloud first policy and going to the cloud, could you just unpack for us how much government data is not in the cloud and is it safer there or is it riskier the fact that it's not in the cloud?

>>Louisa Joblin: Thank you kia ora koutou, in my preparation for this what I identified is about a third of government data at the same time is sitting in the cloud, so about two-thirds is not. And I think there are some very real risks with that two-thirds that's sitting outside in on premise storage, or in hard copy, duplicated, who knows where and by whom and how it's protected.

I think that means that at least thinking about the short-term benefits and the other two panellists can talk to some of the real concerns, but there are some unrealised material benefits to getting that two-thirds out of wherever it is now and into the cloud, in terms of resilience, in terms of security, in terms of privacy protection where it relates to individual data.

>>Phil Pennington: So in terms of those risks and sovereignty, does that come into the mix? How does that come into the mix, because the stuff that is sitting here that's not in the cloud, you've got more control of it or not necessarily?

>>Louisa Joblin: I don't think necessarily, it would depend entirely where it is and how it is. I think the idea of sovereignty if you've got many things in many places in many formats, I would consider that's really quite a barrier to sovereignty. Te Taka can speak to that a lot more, but I would say that is not furthering the idea of sovereignty at all.

>>Phil Pennington: What do you other two think if we're talking about security, remembering we're thinking the short-term problem is data everywhere, Lou said there's lot of government data, I thought there was a lot smaller than that in the cloud, two-thirds is not in the cloud, which is a lot. Is that -- the imperative thing, the first thing we should be doing here is getting it into the cloud?

>>Te Taka Keegan: I don't think it's an imperative we get it into the cloud. For me, I think the imperative is that Māori have control of Māori data, whether that's in the cloud or whether that's in their own servers on their own sites. That's one of the issues at the moment in terms of Māori data sovereignty, there's no real Māori data sovereignty because Māori don't have control of these data.

It was interesting listening to Michael earlier, because he was identified in terms of security risks, identifying which of your data is Māori, well, my perspective is that's okay to identify it, but so what, what are you going to do with it? Māori data sovereignty is giving Māori control of their data, whether it's located locally or whether it's located in the cloud.

The issue with the cloud is, there's avenues and opportunities for other agencies, other countries to have sovereignty, have control, have access to it where there isn't the same issues if you have in-house stored data, and that's a danger as well.

>>Phil Pennington: So you think that security-wise that's a lesser thing and you can deal with that without having to default to the cloud is basically what you're saying? If the cloud is problematic of sovereignty, don't go there?

>>Te Taka Keegan: It depends where the cloud is. The cloud is problematic for sovereignty if the cloud is off-shore definitely because then you're liable to laws and regulations of other countries. But if the cloud is based in New Zealand, then there's more opportunity for sovereignty, but then as well, who owns that cloud, who has control of that cloud? Ultimately as Māori we'd like to see Māori clouds residing in New Zealand that Māori have control of. That's tino rangatiratanga.

>>Phil Pennington: Thanks so much. What about you Don, we have a problem data is coming out our ears, isn't the government struggling to keep it secure which is what Lou's point is, the first job is to not lose it and get it hacked or whatever, isn't it?

>>Don Christie: I say this as somebody that owns a cloud company amongst other things, you have to define what a cloud is. Basically a cloud is a bunch of computers sitting in racks somewhere and to sort of make out there's this magic because we've discovered some new terms or language for computers sitting in racks somewhere, using virtualisation technologies and technologies that allow us to do micro billing per second of use of a CPU or a disk or some networking capability, doesn't automatically make it secure, private under anyone's control.

So I think we've got to forget this idea. Sometimes the benefits of I read something like the cloud first policy, of using cloud are literally just not laid out, there's no dollars and

cents in that document. There's no sense of how much the country will save, or how much value we'll get from using those technologies, which is unbelievable really when we're saying all of New Zealand government data and systems need to move to cloud, and nobody's done any economic analysis of this. It's just stunning.

So yes, with the latest technologies, the latest servers working with the likes of NCSC and GCSB and so on we can improve our security and we should. But let's not make the assumption that just moving to cloud will make things magically better because we know there are SaaS platforms and other platforms sales force and so on, we have no idea what their security is like.

>>Phil Pennington: I never get to interview 200 people at once. Don you were saying you don't think there's been any economic study to do with -- what is it you're saying?

>>Don Christie: I've never seen the cost benefits from the New Zealand government, whenever you ask for that information, from example a GCDO behind the policy, they always say they don't know because they don't know how much individual agencies are spending. We now that cloud usage as somebody that sells cloud is like a telephone bill. You get your invoices for your cloud usage, there's 1,000 different items every text message that's sent is billed separately.

So the opex of running, using cloud is massive. In fact the economic case for building private cloud for government, you'd basically save money 10 to 1 if you have had a private government cloud

>>Phil Pennington: There might be someone from GCDO here or DIA. Is anyone aware of a cost benefit study that's been done on it? Anyone at all? Never heard of it?

>>Audience member: I think we're working on it. I'm just texting Tony Eyles, he's the director of the cloud programme, he'll be coming to the conference very shortly.

>>Don Christie: I met Tony last week and ran this past him and he had no answer to that.

>>Phil Pennington: Tough questions. Tony's coming, maybe we can hear from Tony later on about what is happening. So it's fascinating to know there's not a lot of visibility. This is one of the thing, my job is to get visibility, to ask questions, what I'm hitting this again and again, is that either you can't get it or you refer it on to somebody else or when you get it is redacted which is a wonderful thing, I love redactions.

To the second question, Te Taka, if I were to ask you what are the key Māori perspectives of the Government's previous and ongoing interests in cloud storage by multi-national companies, and I guess at a figure here, Don you probably know more than me, I think you're talking about the high 90s % in terms of overall data, if you take the 33%

or so that government data is in the cloud and that is migrating there swiftly I understand it's in the high 90s of that is within cloud providers who are from the US. So the big three, typically AWS, Microsoft and Google.

>>Te Taka Keegan: So the key -- I guess the key perspective is that the government is saying, in terms of Māori data, we know what's best, we're going to put it in what we think is safe and it's kind of against Article 2 of the Treaty, so Article 2 of the Treaty Māori have tino rangatiratanga over Māori taonga. So we consider data our taonga. So the key thing is well, Māori should have a say where Māori data goes but it's not even a consideration.

Like I said earlier, Michael was talking about we should identify where our Māori data is, but there's still no opportunity for Māori to have authority, sovereignty, tino rangatiratanga over that data. Because for a whole bunch of reasons, and Māori don't trust the government to look after its data. But we don't have an opportunity to have a say in it.

>>Phil Pennington: What would be one thing that you could need to even get to see it, like how visible is it, what is held and what is Māori?

>>Te Taka Keegan: I don't know how you could get to see it, but there are examples of repatriation of other taonga. We've got repatriation of taonga from museums, why can't we start a process where we're repatriating data, returning Māori data to Māori control, Māori access.

The other thing is what's special, what's unique, what's important to Māori isn't necessarily what's special, unique and important to the government. So Māori can't trust government to see data in the way they see it, so we can't trust them to look after. So really it's the call. We feel we can look after it, let's start repatriating the data. If there are elements of the data that the government needs then ask the different individual iwis that hold that data

>>Phil Pennington: Would that require, to repatriate it, would you have to have a Māori controlled cloud provider to repatriate it to?

>>Te Taka Keegan: Yes.

>>Phil Pennington: Is there one?

>>Te Taka Keegan: We're working on it, there will be one in the very near future. I don't think it's a very difficult thing to do, we're confident that we can do that are so yeah.

>>Phil Pennington: Once it's set up, if you were to go to -- think of going to stats or something and say can we have the Māori data you have to put into our cloud and to take it out of where you control it, because is that what you would want, it's not held and you get a copy, you actually get the whole thing?

>>Te Taka Keegan: That's Māori data sovereignty, Māori having control over their data, that's exactly it.

>>Phil Pennington: Do you foresee a problem with that from the government side?

>>Te Taka Keegan: Yeah, because I don't believe the government thinks Māori have the capability, capacity to look after their own data. Yeah, so I do see a problem, I do see the government having a problem with that.

>>Phil Pennington: Lou is I can bring you in here. We're talking capacity, security and privacy there, any thoughts, any comments on that?

>>Louisa Joblin: I think the cloud first policy is really aspirational, there's a real difference between government data, the stuff the government is interested in protecting and then more from a point of view from the agencies within the government, the humans, the data points behind that.

I guess I can see some really in your face technical issues with removing some of the data and putting it somewhere else, because of that separation between data as stuff that's important to the government, versus personal information that actually relates to the humans that sit behind it.

>>Phil Pennington: So is there a middle ground? I do recall a GCDO, I think it was GCDO report, you might know this one Don, that said, I think it was a report they might have had to do again, maybe it wasn't a great report, but it said that Māori were interested in a partnership, so in other words Māori wouldn't run the cloud platform but they'd get Microsoft to do it but they'd partner up and somehow have control of it. That's what was being said in this thing, it was about two years ago, 2020 report something like that. Does that ring any bells and is that an option?

>>Te Taka Keegan: I can't remember the report. Māori partner with Microsoft, a couple of our major iwi partner with Microsoft at the moment. Personally I'm not sure if that's a good idea. I feel that everything that Microsoft can provide, we can actually build it ourselves. But we can build it from a Māori perspective. Then when Microsoft don't want to do an upgrade or want to change it, charge us a little bit more, we're not under that control. So my personal perspective is partnering with a large international organisation in theory sounds like an easy way to do things but in the long-run it's detrimental, let's just build it ourselves.

>>Phil Pennington: Don you've been building this stuff, can you comment on necessarily, I think there's a core question, a trade-off here, that if you want the security for Māori data or any data for instance, that you necessarily going to trade-off if do it locally or you do it small

with sovereignty, because you're going to gain sovereignty but you're going to lose security because the big guys know how to do it better. I'm only a lay person, I would have thought the big guys do know how to do it better because this game is scale isn't it. They've got more data and more tools, they get to play with more stuff.

>>Don Christie: So you heard from NCSC earlier today, New Zealand's a tiny country. The idea that we're hyperscale is a joke, we're kind of 0.16% of the world's population and 0.34% of its economy, we're not a hyperscale country. So the approach we can take to cyber-security is national and local and community. We have that opportunity.

The technology as well, if I look at the technology behind Catalyst Cloud it's open stack, completely open source, it was born hyperscale if you like, it was born out of NASA and CERN with the large hadron colliders, it's used in the NSA on tens of thousands of hypervisors, but when we brought it to New Zealand when we were first doing our proof of concepts over ten years ago, we were running it on laptops because it can scale right down as well. So to pick up on the earlier comment about building local capability, research capability in a rohe in the areas where mātauranga Māori applies which is very, very local is absolutely the future of cloud computing.

And this is where something like the cloud first policy is just completely missing on the vision and opportunity. It's the opportunity to enable Māori and the rest of New Zealand, data sovereignty isn't solely a domain of Māori, we're dam lucky to have people like Te Taka leading this conversation, it's a concern to all of us, to the rest of the world

So we shouldn't just park the idea that yes if we solve it for Māori we can then forget it for the rest of us. We all need to be Māori about this and be concerned about it. One the technology is going in a direction that absolutely backs up what we've heard about what capabilities can be built. Two New Zealand is in the unique position to create a cyber-security framework that would protect our manufacturers, protect our communities and protect our small businesses

>>Phil Pennington: How much longer have we got? We want to leave some time for questions from the floor or virtually. 15, that's fine okay.

>>Te Taka Keegan: Can I make a quick comment?

>>Phil Pennington: Go for it.

>>Te Taka Keegan: Earlier today there was a question about whether you're able to use AI in your company or not. The thing about using AI in your company was it was feeding all

your information back to the mother ship. Why don't we have an AI system that cuts off from the mother ship and then we use that in our company.

So last night I was talking with one of the researchers at Waikato University and he had a version of AI running on a five-year old laptop and it wasn't as fast as chat GPT, but it was pretty good and it was responding in exactly the same way. So rather than fear the technology, I think it's better to use the technology for our benefit.

So the example we have at the moment is that chat GPT works really well for te reo Māori, it's like how does it do that, how does know? It works on data, it's managed to get a whole lot of data, where does it get that data from? I know where the most largest Māori language kopa(?) are in New Zealand, I know they're not sharing them with Open AI. But most of its data, 66% of its data it gets from trawling the web.

So then we're thinking let's run a version of a Māori chat GPT that's not able to crawl the web but able to crawl Māori actually data. Specifically iwi data, let's have an iwi data chat GPT that isn't feeding stuff back to the mother ship, that doesn't need to be cut off, that we can use it for our benefit.

So really I think it's about understanding the technology, understanding the flaws in the technology, but turning around, using it for our benefit. But also not having to be reliant on some big overseas corporation as our saviour. We can do this.

>>Phil Pennington: To pick up on that, remember we were talking about trying to fix short-term problems, whether it's delivering us a long-term road that we don't want to go down in terms of sovereignty. To reflect back it's possible if we were to take you on good faith that you can build this stuff locally, it can be good enough for security so we don't have to trade-off and we don't -- then we have to grapple with the sovereignty thing.

Where we're at, decisions are being made above whatever level they're being made, maybe some of you are making these decisions that are privileging certain things. I know for instance there are memorandums of understanding that the government has with Microsoft and they signed up with with AWS. Is there a memorandum of understanding with any local cloud provider Don?

>>Don Christie: No.

>>Phil Pennington: Don't know why. The government made that choice. We see Microsoft, I'm just looking at OIA now, in mind it the Ministry of Education discussing -- this is under the MOU that came out from Microsoft -- which by the way was not made public at the time, we only found out about it because AWS thankfully mentioned that they had one. Then we went asking for the other one and we got that, I think it was a couple of years old and it has

things like a project with the Ministry of Education to look at the use of AI in schools, which the Ministry of Education was very -- no, we didn't do that. Looking at the OIA on that, one of the things it talks about is getting data from neurodiverse students and giving it to Microsoft. Haven't reported on that yet.

What I'm getting to is there are decisions being made, paths being trod, so what I want to get to and starting with Lou -- no we'll start with Don this was your question, we'll come to you Lou second. If we stay on this where you think we are, because we all think we're different places, if we start with where you think we are, 25 years hence where are we going to be at? That was your question Don.

>>Don Christie: Let me unpick the comments beforehand. So I'd like to look back to try and inform the future and you mentioned in the start I was brought up in Zambia. I was born two years after that country became independent and our first president was Dr Kenneth Kaunda, whose philosophy was as a humanist, that was how he wanted to run and govern the country, a very people-centred philosophy. He would be inspired by people like Mahatma Gandhi who spent his early life in South Africa and would have been dealing with the people in the ANC and so on. Mahatma Gandhi was inspired by Te Atiawa, the people of Parihaka. So here we are coming around full circle, where Māori leadership and thinking and philosophy back in 1860 to 1880 led the world in thinking how you unpick an empire. Can you imagine that. That thinking led the thinking about how to unpick the biggest empire the world had ever seen.

Māori thinking now is leading us on how we think about the future of data, of digital sovereignty, of cloud. And the rest of the world is following. The rest of the world is looking at this thinking, they're looking at mātauranga Māori, knowledge systems, how we want to treat data, that our communities want. The technology, as I said earlier, is behind that. We're ready to go. We can build the local cloud capability for tens of thousands of dollars, not even hundreds of thousands. We can federate those local clouds.

So they come under the governance of the people for whom those clouds have been given and who can serve their communities, but then when it's important to share data maybe for ecological reasons for whatever the purpose of the data was gathered for, to share that data so it creates that greater purpose. That's what we can enable. That's what the world wants and that's what it's looking back to New Zealand for again.

So as I said earlier, I think we're really lucky to have people like Chris Cormack, the (te reo Māori) group, to have Te Taka here and so on, we're incredibly lucky and the rest of the world is watching us **[Applause]**

>>Phil Pennington: Big question, before we take questions from the floor, Lou from a legal point of view do you see problems? When you go down a track you sign contracts, aren't we locked in now?

>>Louisa Joblin: Do you mean with Microsoft and things? It's hard to say not knowing the terms of those contracts. That could be a real concern that we've committed, who knows for how long and on what terms. I guess I would be hopeful that we have retained the ability to do other things. To my mind a memorandum of understanding doesn't sound like a be all and end all agreement, but I don't know, really I don't know enough about the terms.

>>Phil Pennington: I suppose the MOU is like turning over the garden and it's what you sow in it afterwards, but it is getting sown with those seeds that are for that. And the trouble now is you'd have to be go digging another garden somewhere else and the government, there's not the resource. What do you think? It's hard to see it changing.

>>Louisa Joblin: Yeah, I think at a take a step back level in terms of the relevance for the people here, none of that takes away from the agencies, the ability to plan and prepare and put good measures in place and have, as Mike was saying before, have a plan so that none of this is a surprise, you still have that.

Q&A: Security and Sovereignty in the Cloud

>>Paddy Power: I do think we need to move to take some questions from the floor Phil, before we go too far. I've got some from Slido but we will take questions from the floor. If you've got a burning question, you want to hear your own voice rather than my voice ringing out on Slido, put your hand up and we'll -- my colleagues over there will give you a microphone.

First question on Slido is, I'm not going to read that first question. The answer is no. What are some current examples of Māori having control of Māori data, originally held or gathered by the state. Do government agencies understand what this means?

>>Te Taka Keegan: That's kind of the issue, I don't think there are any examples. I don't know any data that's been able to be repatriated because I don't think the government has faith in Māori to be able to look after his data, which is quite disappointing.

>>Paddy Power: I have an example that might be relevant, because I work for Stats NZ, when we publish the iwi affiliation data I think it was last year we published it, we released it on Te Whata at the same time, possibly even slightly before it was released on the Stats NZ website, that's not exactly the same thing, but I think we're trying.

>>Te Taka Keegan: Yeah, okay, thank you.

>>Paddy Power: Any hands up in the audience? No? How can we say we don't know the security of sales force and other vendors when they can produce SOC turn(?) audit reports every year?

>>Don Christie: Anyone remember Solar Wind? Anyone impacted by Solar Wind? No? So that was the software that a lot of agencies in New Zealand and across the world used to run their Microsoft frameworks and desktops and so on. That was subject to a very serious hack earlier this year, it was audited and certified up the wazoo.

If you read the cloud first policy, one of the things they talk about with data centres based in New Zealand is that you can physically audit them. For eight years we've been physically audited by defence agencies, by DIA and by our clients. The level of audit that can take place close in the supply chain is really important.

And it's another layer, it's -- there's no panacea, there's no perfection. I suppose what frustrates me about sales force is I keep hearing of another half $1 billion going to go on a sales force project. There's one just the other day I heard about coming up and I kind of think what an earth are we doing? It's a CR M, how hard can it be to spend 20 million and build in New Zealand and certify and deep our health, water data, this fantastic data in New Zealand under the control of whoever we want it to be under the control of?

>>Paddy Power: One more question here. How do you know what data is Māori data? Many organisations don't really understand how to do this.

>>Te Taka Keegan: The Māori data sovereignty website actually has a definition, I don't know the definition off the top of my head, but it is there. But it's along the lines if it's data from Māori or about Māori, then it's Māori data. So that's quite simple really. If you're collecting data, a whole bunch of people and in that organisation some of those people are Māori people, then you're collecting Māori data.

>>Paddy Power: I think we've run out of time and we need to let our next speaker. So Phil if you want to sum up.

>>Phil Pennington: Yeah, well thank you very much for that fascinating -- I hope that it was enjoyable and also educational. Thanks Lou, thanks Te Taka, thanks Don and I've really enjoyed it.

Just before I go I want to give examples of where things, some things have gone. These are real life examples or proposed examples. The Police. So they store evidentiary data that is also processed, not just stored, but processed with a US company that stores it

in Australia. So that's a company called Axon, so there's data that's evidentiary data as well from family violence cases that's going to Australia. Security, sovereignty problems.

The courts of course are going digital, they've said that they will probably use the cloud and they haven't ruled out it going to Australia. But even if it stays in New Zealand at one of the new hyperscale centres it's likely to be owned by our friends here or Google and Microsoft, not Google, they're not in the data centres here.

The final one would be Waka Kotahi. They're about to bring in the national ticketing system which will have a lot of data about you as a traveller in it. That contract is being rolled out by a US contractor with lots of experience in transport and defence, it has contracts in transport and defence and with security agencies in the States. Thank you. **[Applause]**

11:25 am - 12:00 pm: Institutional Resilience - From Customer Service to Crisis Recovery

- **Damon Rees**

>>Paddy Power: Thanks Te Taka, Lou and Don. Here's a small gift, it's really the ability to donate to a charity to your choice from GOVIS. Thanks **[Applause]** I'll introduce our next speaker. Damon Rees is -- Damon begged me not to read all of the information in his profile in the programme, so I won't. But he is a business leader focused on customer centricity culture, digital enablement and innovation with more than 20 years experience driving transformational change, organisational performance and better customer outcomes. And Damon's keynote -- he's talking about Better As Usual, institutional resilience from customer resilience to crisis recovery. We're very thankful that Damon is sponsored by AWS today.

>>Damon Rees: Good morning everyone, my name's Damon I join you from -- I live on Wangal land in the inner west of Sydney grew up in the Blue Mountains. It's a privilege to be here, I'm not going to talk about Better As Usual at all, six months into the third chapter of my career, first chapter of my career was banking and corporate, the second chapter of my career was public service and I'd like to talk about that. Every time I'm in the room with fellow public servants I'd like to say thank you, I think the work you all do is profoundly important, profoundly impactful and not always appreciated to the extent that it should be by people outside of the public service. So thank you for everything you do.

I'd like to talk about Service New South Wales. I had two roles in the public service, the first was to lead digital and technology for the New South Wales government, the second is the chief executive for Service New South Wales for the last five years. We were having a conference around resilience, there's a couple of stories I think we can really bring out and share learnings and insights from when it comes to service in New South Wales. I'll talk a bit about the why, what, how to give you a service of New South Wales and we'll touch on resilience and we'll have time for questions.

I'm in the wrong spot, do you want me to start again? No. But before I get into that we've got a little video, excuse some of the effervescent language but it was a 10-year birthday celebration for service New South Wales, for anyone who hasn't interacted with it 2 might give you a sense of what we're talking about before we go forward, can we get that video played please. **[Video played]**

So hopefully that gives you a bit of a sense as to what we're about. Standing invitation, anyone finds yourself over our side of the ditch please let me know and we can arrange a few visits, it's really special. I'd like to go back 10 years and start with the why. For us this is really about enabling our state government to have the greatest impact that it could have and to fulfil its purposes at state government

Our view was actually that ability is underpinned by a couple of things, by trust in government, and trust from communities and trust from the people that we're here to Serb. It's underpinned by the ability and the willingness of people to engage with government services.

We recognise actually tightly correlated with that is the experience you have with Government when we looked at experience people in their lives in Australia, and if you ranked them from best to worst, government was right at the bottom of that list. If you look within government and ranked all of the governments in Australia from best to worst I think we were second-last in New South Wales and only ahead of our Commonwealth counterparts which is not really a whole lot to crow about at that time

So we thought this is something that needs to change, if we don't change there's that gap between the experiences that people have in every other part of the their lives and the expectations they bring to government is going to get wider around wider and that will erode the trust in our constitution

That's why Service New South Wales is created, how do we move from an agency-centric experience of government that really doesn't think about the experience or prioritise the experience or think about the people that we're interacting with as customers

and through that lens, how do we turn that on its head. That's where Service New South Wales was created

We started as a new agency in government for really two reasons. One was we were trying to introduce a different experience of government, a customer centric experience of the whole of New South Wales government not just a better experience of individual pieces

But the second and I think the most important was culturally. We wanted to create a very, very different culture that underpinned that experience that people had of New South Wales, our view was we didn't see that existing in government anywhere and we wanted to start that again, build the DNA of the organisation from scratch

That new organisation drew people in from all sort of walks of life and all sorts of professions, from hospitality from, airlines, the banks. Importantly, though, to this day about half of the frontline team from service NCSC also came from other parts of government. Many of them came from the parts that people referred to disparagingly and contrasted with what they experienced through Service New South Wales. So it's not about a story about none of the people we have are the right people, it's a great example if we can change the conditions around our people, the environment around our people, if we can change what really matters as government actually we really do enable a lot of the people that we have today to blossom and to be part of that journey.

So we started as one service centre ten years ago in a little town called Kiama, a couple of hours south, got the concept right, showed what a really, really different experience of government would look like. And then just learned continuously and iteratively to the point where we now have 114 of those wonderful service centres through the state. We have mobile service centres, we have contact centres, we have a digital experiences that's getting richer and richer, and a fabulous mobile experience

People often talk about Service New South Wales as an example of transformation. I tinned to think of it yes, but 20% transformation and just this re lens less learning and evolution and execution to keep building on that.

If you think about what sits between the scenes, often we look at the outcomes that organisations achieve, we think we like that, we don't like that, we like this organisation is sustaining these different things. I certainly found through my time at Service New South Wales in order to achieve those outcomes and keep sustaining them we really had to object sense around the enable letters of that. It boiled down to a handful of things we spoke about as our leadership obsessions. The first would be customer centricity. A lot of organisations talk about it for Service New South Wales it was woven into every single

conversation, every conversation was brought back to what is this going to mean for our customer what's this going to mean in the context of their life. It really did term permeate our decision-making in a rich way. It got us thinking up above and beyond ourselves. If we were having a conversation around risks that we were taking on, it wasn't contained to what does this mean for us as leaders or Service New South Wales as an agency, what are the implications on our customers if we don't take this risk. In order for us to reduce our risk, do we transfer a greater risk on to our customers.

Customer centricity was brought to a life in a way that's deeper and more pervasive an any organisation I've had the opportunity to be part of. There's a range of things we did there I think at its core it was a very plait very open high trust organisation, so that voice of customer constantly washed throughout organisation. We had a culture of really trying to empower our team. My view is always that the best person in our organisation, there are a team of 6,000 by the end, the best person to make the best decision possible for our customer is not me it's the person that's closest to that customer, typically the person in front of that customer. So we were constantly working to say how do we empower and enable that culture through our organisation and the team of our organisation.

We had programmes like service time that enabled anyone in the organisation, including myself or our stakeholders to not just go and experience the frontline and to spend time with our frontline, but to put the wardrobe on and receive some training and go and spend a day serving customers. It made sure that empathy and that connection and understanding wove right through our organisation. Then we started bringing friends from Treasury and friends from other partner agencies, I think it was one of the things we were really able to provide a value to the sector was a way to connect all of the great work that was happening across the sector with the true outcome and the person and family and community that were at the end of it.

Customer-centricity absolutely key, we nurtured it every day. Hand in hand we focused on our people, we can't be great for our customers if not great for our people. We focused on how do we make this a great place for people to work. We pushed ourselves further than that after a while and said how is your life better with Service New South Wales as part of it than without it. How does Service New South Wales be a place that is enriching and rewarding and full of purpose, a place that gives you personal and professional development, a place where you can be surrounded by rich relationships and where you have the support when you need it.

Everything we see culturally, everything our customers experience, is intertwined with that commitment, that genuine commitment we had to our people. Service New South Wales has the highest engagement scores of any large agency in New South Wales public sector and was the first organisation from the public secretary to be to be recognised as a great place to work a number of years ago

The third thing we focused on was our agility. I don't want to use the language agile and have people suddenly make automatic connections to methodologies and religious wars and stand ups and Post-it Notes. But age I will tea at an organisational level in the truest sense. Our reflection was that it's wonderful our customers receive this one stop shop of New South Wales government but if you look at that from the inside out we're in every agency supply chain, every one of those agencies has ministers that are trying to get things done, they've got commitments, policies, if we're not by some measure the most nimble and adaptable part of government we're going to quickly become the bottleneck of government. That would put a ceiling on our ability to keep growing our impact and our value for our customers. Agility for us was an obsession. It forced to us rethink many aspect of who we were how we worked and how we did what we did. We had to pull apart old architectures, to construct new ways of working, needed to build new skills in our organisation. A critical part of what's enabled us to continue to grow our value, as we get to resilience in a moment, a critical part of what enabled us to step in to spaces we'd never anticipated being in, but make a real difference.

We focused on partnerships, so Service New South Wales in the early days had wonderful customer satisfaction but didn't have a great relationship with other parts of government, there was a real tension there that was ultimately getting in the way of our ability to not just deliver a great customer experience but to deliver a great customer outcome, to work through the processes and policies and the hand-offs end-to-end to make sure every part of that came together as well as it could for the outcomes and people we were here to serve.

Partnership satisfaction, when we first surveyed it customers 97 but partners were 13% from memory. That now sits at about 80%, we had to change the way we do that. I think it's now become part of the secret sauce, there's a wonderful high trust, collaborative relationship between Service New South Wales and the many parts of government we partner with. We do very little completely on our own and independently, almost everything we do is done in partnership and on behalf of another part of government that

will ultimately own the policy, responsibility and outcome. That partnership is absolutely critical for us

Digital capability. When I joined five and a half years ago we looked a little bit like most other parts of government in New South Wales, we had a lot of passion and energy which was the Service New South Wales way but we had a small tech team that designed stuff up and specced it up and took it out through procurement, a partner that designed it, built it, ran it. We couldn't get out of first gear, we couldn't do many things at the same time, we couldn't move at the pace that our customers needed to.

So how do we rebuild and rethink this as a core capability of our organisation. How do we change our minds so the person who designs and builds and owns the experience our customers have digitally recognise that just as core as the earn person who greets you. These days the digital team in Service New South Wales sits at 5 or 600 people, it's all built on lean agile cross functional teams it works at a face like I haven't seen before and it's constantly pushing itself further, a key part of what's enabled us to do the things that we've done.

So I might then bring us to a conversation around resilience, I didn't want to start with resilience without giving you a sense to where we started and what sits behind the curtain. Because we started very much focused on the transactional services of government, we're going to make it easier, give you a one stop shop on the transactional services of government, registering this, renewing this, paying for that. We're going to focus on the individuals first, business, communities were in our thinking but they weren't the priority.

So we then found ourselves in 2019 from memory we were coming in, maybe it was 2018, the time starts to blur, bush fires were ravaging New South Wales, really, really traumatic for families, communities, for the state. And as the fire fighters started to get on top of the fires you were left with the devastation of communities, the question of how do you help individuals, businesses, communities, recover.

Our culture meant that we automatically put our hand up, is there anything we can do. We can see our own teammates are impacted by this, we can see our customers are impacted by this, the communities are impacted. We'd had no role in disaster recovery up until then, we stayed can we help. There was a cautious look there's a spare table over here in the recovery centre, come in, all right, see what you can do

One of the great things about the bush fires was everyone wanted to help. It was really, really humbling. But if you were a customer that's just lost your home, or sometimes

a loved one, it was overwhelming. The situation you were in was overwhelming, your ability to navigate that support and work out where to start it was just beyond many of our customers

And so almost overnight we said we think that's where we can help, let's create this customer care service, let's make it a relationship managed service so you can deal with the same person over the days weeks months that you're going to need as you go through your own sort of personal journey of recovery. Our culture got us automatically stepping into that, our capability in our frontline meant we just went in there without any playbook, without any rules, without any policies, we have this problem-solving muscle, this incredible empathy and care in our frontline, that's where we started then we raced behind the scenes to industrialise it, how do we get the systems in place when Damon's not here, there's someone else that can smoothly handle it. How do we start to bring in the digital experience for those customers that don't want to or aren't able to get themselves to a recovery certainty. That's where that digital capability and that agility of the organisation kicked in

So we found through these capabilities we had, these muscles we've been building for years we were able to step into these spaces. When we first did it for bush fires we were on the edge. Fast-forward a few crises later for northern rivers flood, Service New South Wales is the primary way that government steps in and not just supports customers now, with others, it's not only Service New South Wales, not only supports customers but we've become the primary way government delivers outbound support. For our first seven years we just really received money on behalf of government through fees and fines and that sort of thing to the tune of $7 million a yeah. For the last couple of years we paid out $14 billion in the form of grants for bush fires, Covid, floods, droughts, mice plagues, the list goes on

None of that would have been possible if we hadn't had this cultural willingness to step into the grey and the unknown in the space. If we hadn't had the agility to back ourselves in and the digital capability to really industrialise behind the scenes and bring still a

People would say to me you're running this organisation, what's the vision, where will Service New South Wales be in five years' time. I used to slug, my answer annoyingly for everyone was guys we'll be where are our customers around state need us to be. What we are going to focus on is making sure we have the adaptability, we have the internal

resilience, the capability to be able to adapt as an organisation and as a team and go where people need us.

And that's where we are today. I finished up after five years at the end of last year and I could only see unlimited potential ahead for an organisation like Service New South Wales. I think all of you in public service can see there is, and I suspect always will be, an unlimited amount to be done. But what I love is the fact that Service New South Wales has those core attributes, core capabilities, that adaptability that is enabling us to continue to step in

The final thing I'll touch on then we'll go to some questions, I'd love to open up the conversation. But in order for us to play that ever and more impactful role in the resilience of our state, we needed that same focus on our teams and our organisation and ourselves individually and as leaders. Making sure anyone who's in a situation where you're trying to lead your team into difficult times or for many of us coming out of Covid into a strangely difficult time. There is that piece around how do you look after yourself just as much as you're looking after your teams.

I'll just pause there, I'd love to see if there's any questions and take the conversation where you'd like to go.

Q&A- Institutional Resilience

>>Paddy Power: Thanks Damon, we've got some questions on Slido K we put those up. Who provides the software for Service New South Wales, very practical question.

>>Damon Rees: Great question. Our digital experiences are built internally within Service New South Wales. We have lean agile cross functional product teams with product management design and engineering, we tend to build those solutions using full stack techniques. We leverage cloud capabilities. For us largely for the elasticity and the agility that used as programmatic infrastructure that provides us with. We have a very strong focus on devops and continuous development. We've got a very strong focus on developer and development productivity enabled through a range of digital platforms.

>>Paddy Power: We've got questions moving up and down here. How do you promote a culture of allowing your teams and people to start somewhere and possibly fail and continue to grow and iterate?

>>Damon Rees: I remember when I joined, I joined government from Macquarie and it was my first week in government and wise end government folk sat me down and said we've got to

tell you how it works here. They said you've got to forget all of that fast fail rubbish that you've learned in the private sector because we're government we don't take risk and we can't fail. One of my responsibilities at the time in my first role was investment assurance for government, it was set up because government had had a programme that had run half a billion over budget and ended up landing six years later delivering something that didn't do the job and no-one wanted.

So my view was because we need to reframe the way we think about this. Actually learning and experimenting is about reducing the risks we can't take, rather than taking risk. If we've got an idea and we spend a month and spend a few thousands dollars and test it we realise it's a bad idea and we stop that's not an interesting headline for anyone to read. If we don't do that experiment and roll forward on the wrong path for five years waste half $1 billion of taxpayer money and deliver a rubbish outcome that should be a headline, and that's a disaster.

So I think reframing some of these conversations would be my view. One of the secretaries I work for, people talk about government being risk averse, and they said we're not risk averse we're risk blind. So I think really trying to open up the conversation and see it through a different lens would be my little thought there.

>>Paddy Power: Now a question about governance. What kind of governance enabled that transformation you were talking about?

>>Damon Rees: I don't know how to answer this question neatly, it's a great question. We had very strong sponsorship in Service New South Wales and I think there's -- if you think about the things that helped Service New South Wales start versus continue, those things move around over time but certainly I think there is a very important role of sponsorship to get going on something like this. Governance probably the key aspects of governance that would be worth flagging, one is we really deliberately tried to keep things small. Our view is we were most successful when we had six months to do something. If we were given two years to do something very quickly we let ourselves over-complicate things and we were less successful. So we had a very deliberate focus on moving quick, maintaining constant momentum. We delivered everything in partnership with other agencies, so when we'd come to governance very strong focus on how do we build that governance together so in combination with transport or births deaths and marriages, whoever it may be we can really jointly govern these initiatives to ensure they're win-win, they're good for customers, that they help the partner agency be successful and achieve their policy outcomes and that

they are coherent and work within this overall experience of government that Service New South Wales is trying to do.

I think my final comment on governance, this is not a complete or neat answer, but we were the opposite of a hierarchical organisation. Incredibly flat, everyone had had a voice, and we were -- we actively sought out and listened for the voices that were different and the voices that were most close to our customer.

>>Paddy Power: Thanks Damon. This is one I'm particularly interested in. How do you avoid failure demand? You've got phone lines jammed with repeat calls because you're not making it easy for people to fix things themselves.

>>Damon Rees: Our view is there's a huge pay off. If you look at many organisations the amount they're spending to keep resolving the work that failing to do something right the first time creates, I think the hard thing is how do you create the space to get ahead of it then I think it very quickly becomes a self funding proposition.

In our organisation that was just about managing our priorities. We'll take a little bit of short-term pain, we will pull capacity and make capacity available to sort this stuff out, and a belief that actually if we get the outcome right for the customer the first time all of that work is never going to exist downstream. There's good research out there around the escalating cost of not getting something right the first time. For us it's a great example of -- things like great customer service and great value and being lean and evenings, these aren't sort of in tug of war with each other, I think there's often a false dilemma we're confronted with in government, do you want it good or do you want it cheap. I think in areas like this the answer is the same. If we can do it really well and if we can do it really well, the first time that is also the cheapest possible way for us to do something.

So I think it starts with a mindset and a belief. And then it starts with some good old-fashioned reallocation of your capacity and your focus to enable you to start to break the back of the things that are clogging up your organisation.

>>Paddy Power: I think we'll take another couple of questions, so if you look on Slido and there's a question you really like, give it an up vote now. I see we actually have a hand up in the room.

>>Audience member: Damon, this is a question about digital equity and trust in government. So you've painted a very nice picture of one place, one source of the truth, 85% uptake, the one place to go. What about the challenges of people who either don't have access to digital, so that's 15% maybe of the eight 5%, or people who don't like the idea of my ID and my Covid pass and all my data, are we leaving people behind and how do you solve that?

>>Damon Rees: Great question and really close to our heart. Former teammate of ours Kylie quipped this for the first time which is hey folks it's in the name, we're Service New South Wales not service some of New South Wales. And so for us that was right in the core of our culture, how do we make it easy, how do we help every last person and now every last business in New South Wales.

There's a whole long conversation around all the things we've done and are doing and importantly a constant focus on working out what we could do more. The first thing I'd say we're an Omni channel construct. You'll never hear language from us around digital first, not from me anyway and you'll never hear language about drive to digital. How do we make it easy for our customer to get the outcome they need. Our customers are diverse, so for some people the easiest way for them is on the couch on their phone at home. For some people the easiest way for the same thing is with one of our teammates in a service centre. We have those 114 service centres, we have mobile service centres that take everything we can do in a service centre into even more remote and regional communities and can drop all of that into crisis impacted areas.

In our service centres we have digital kiosks, we have team members that can help you. So for people that -- the gap is different for different people. For some it's I just literally don't have access. So we consider our footprint across the state as a bit of a bridge to minimise that digital divide for communities that's around access. For some it's I have access but I don't have confidence. That's where our teammates kick in. Actually some of my favourite conversations to overhear in service centres are our teammates helping customers set up their first ever email account, explaining to them about things that had nothing at all to do with us but helping them build the confidence and the engagement in digital

So excludes can be about digital, can be about accessibility. Last year we introduced quiet hour, so our service centres are energising, but if you have autism, that's not a positive, it can be the difference between whether you can pass your learners exam or not. So we created a low century sensory experience called quiet hour that was better suited to the needs of some of our customers. We're constantly working to say how are we more welcoming, inclusive and understanding of our Aboriginal and Torres Strait Islander customer base. The job is never done but I think Service New South Wales sees ourselves as playing a key role in trying to fight that unconscious exclusion that can creep in in this kind of what tends to be sort of a digital first mindset that's permeating lots of places.

>>Paddy Power: Final question is the one up on the top there, how do you feel about using the term "customer" for the people who use Service New South Wales? Is it more accurate than "Australian" but does it sound a bit commercial?

>>Damon Rees: Yeah, I love it. So Service New South Wales about a year, three years ago now became part of a bigger push called the Department of customer service. The language was introduced in New South Wales government, 11, 12 years ago, really deliberately. And it was jarring and uncomfortable language for many parts of government. That raged for years and years, that's not a customer that's my regulated entity. They're not a customer they're a voter or a citizen or a prisoner of Her Majesty's, whatever the language is.

The language was helpful because we although what good customer experience looks like and feels like. We although when we've had it, we although when we haven't had it. So we used it as a tool to shift culture and to create a public service that thought about the person that we were here to serve, thought about the impact of serving or not serving that person, thought about the quality in which we did or didn't, thought about the whole life of the person and the impacts of our engagement on that person and the community. It was a cultural lever.

And what I would say, I joined New South Wales government probably 3 or 4 years into that customer -- when I got there maybe we were 50/50, there's a bunch of people that embraced it and there were still maybe half the government that was kind of wriggling and uncomfortable.

By the time I left it was not a conversation anymore. And I'm not saying Police ran around calling everyone customers. But that cultural mindset had really permeated far and wide. I think that was -- that's the power in the language. If there's a better word, use it. But for us it was a tool to start that cultural shift. And that shift has had very, very, very far-reaching I think consequences for New South Wales, far beyond how friendly is the person that helps you or how nice is this digital experience to use. It's enabled when different agencies are trying to partner together and we get stuck in our own sort of views of what's matter, it pulls us up and gets us focusing on outcome like few other tools we've ever come across.

I think it's helped bring policy and delivery closer and closer together to the point where more often than not now it feels almost indistinguishable around who's around the table. It's seen as reaching for an understanding of actually what is the context and the person that we're trying to impact here, and not just making that kind of with a blinkered view in an ivory tower. I think it's got us thinking about exclusion and inclusion and

accessibility in a way that we never would have before. So for us the language has been phenomenally powerful. If there's better language culturally is going to work better for yourselves, then please don't feel the need to use our language. But think about what is that cultural shift you might be trying to make.

>>Paddy Power: Thanks Damon. That was really interesting talk, it's great to hear from -- sometimes hearing from somebody from outside New Zealand you think -- you hear about things from a different perspective. I found that really helpful. I think it would be really an interesting talk for anybody who's trying to help New Zealand citizens, customers across New Zealand. So thank you very much for that. And we've got a little gift for you which is over there I'll grab it in a minute.

So it's time for lunch now. And so I want to, before you go and get your delicious lunch, I want to do a shout out to our sponsors, OSS Group and IBM for co sponsoring the lunch, it looks really delicious. Thanks again to Damon and all our sponsors. Go and get some food.

12:00 - 12:40 pm: Lunch Break

12:40 - 1:10 pm: Oceania Stream: Lightning Talks - Resilience in IM

Evolution or Extinction? The Choice Facing Information Management - A Manifesto for Change

- **Stephen Clarke**

>>Chris McDowall: Our first speaker for this set of two is Stephen Clarke, and he's going to be talking to us -- his presentation is excitingly entitled evolution or extinction, the choice facing IM, a manifesto for change. Stephen is currently a virtual CDO and information data management consultant. He's originally from the UK and has worked in senior information and data management across the NZ public sector for the 15 years. His most recent role was Chief Archivist after moving on from his role of Chief Data Officer at the NZ Transport agency. He's known as a standards expert and has developed standards for information management for Australia, New Zealand and as an anthropologist Stephen understands human systems, and as a technical expert he understands information systems.

So it's all about getting technology to connect these two systems to get the right information to the right people at the right time and that's his professional goal. So yeah, please join me in welcoming Stephen for this first lightning talk.

>>Stephen Clarke: Kia ora. Ko Stephen Clarke tōku ingoa, I've only got 15 minutes so I'm going to get straight on to it. So yes, I've moved from being a public servant which I've done with a great zeal for the last 20 something years in the UK and New Zealand to jumping the other side of the fence and trying to help government on the other side as a consultant. So hopefully, or I certainly see myself still being a public servant just once removed.

And the theme of this conference is resilience, I thought one of the key things about resilience is learning to bend not to break. And to understand where you are in order to be able to change. I feel that I'm representing -- I'm putting on my global ambassador had for this talk today. I just think we're at a crossroads for the records and information management profession. It is in my view either evolve or become extinct

If we think about the profession, it goes back six, seven thousand years to the Sumerians that started doing proper professionalised structured information management for the clay tablets that we can still read now, and they did metadata and version control, when it's a final version you bake it so you can't change it any more, you want version control you wrap it in a fresh layer of clay so you don't have an alternative version of the truth floating around, and you put all your metadata stamps on the outside side so it's well described and encrypted. We're still doing that incredibly efficiently today and don't have any alternative versions of the truth floating around

If you think to Rome when it became professionalised and they made the distinction between archivists and records managers, things went a bit backwards from the 4th, 5th century, then we come to the modern profession which came out of the change of the French Revolution and the birth of the new nation state and how do we bring information together at a national level and respect the fons(?) and all of that stuff that underpins our professional thoughts.

In that 6, 7,000 years as information managers we haven't had a lot of competition. In the last 50 years we have. The rise of IT world and the IT professions means that looking after data and information is no longer the preserve of just information managers and archivists

Partly what went wrong and partly how do we do something about that. So the world has changed and I don't think the profession's changed with it. I genuinely don't

think our profession has really made the jump from the paper paradigm into the digital native environment.

And we don't speak the language of our partners. We don't speak IT O, we don't speak service delivery life cycle etc etc, so what can we do about that. I'm not going to read this slide out it's pretty self-explanatory. I just off the chat GPT and said hey tell me what are the key challenges for the information profession at the moment. And made it make a bit more sense. But I just thought if you can't beat them join him. I looked at it, this is all stuff that we although, right? None of this is kind of earth shattering or ground-breaking stuff

I do think in aggregation it does present us with I think an existential threat to the future of our profession. I'm not sure we're evolving, I think I'm seeing a bit of an extinction going on

What are we going to do about it? I think we need to change the way we think about ourselves and change the way we present our services and our benefits portfolio out to our customers around how we engage with our professional colleagues. Again I'm not going to read them out but you can see from the principles I'm putting forward they're all very positive, say yes, don't be the Ministry that says no, collaborate, speak the language of your partners.

And we have a lot of skills that we can bring to the table that we've developed in that last few thousand years of working with information and data that many of our colleagues that come from the technical backgrounds don't have, deep ethics, understanding of ontology, understanding of semantics, deep understanding of information and how it works within cultures and systems and how it's an artifact of cultural expression and who we are as an expression of humanity. That's not something you hear an awful lot from IT professionals talking about that. But information and data by its very nature is expressed through language and expressed through ontological and semantic meaning so we understand stuff in a way the machines are now catching up with. That's one of those big differences and big changes that we're up against, which is large language models but is as information professionals we've been dealing with semantics and natural language processing for decades and centuries so we can bring that deep knowledge and thinking to bear but in a different way, instead of being the Ministry that says no, and wagging your finger and saying this is the functionality you must put into M 365, actually think about what is the customer benefit and how do we make that service much more efficient for people so they get a much better positive outcome and hide what we do back behind the

curtain like the wizard of Oz like we used to if you go back pre-1980s, 60s and 70s, no-one knew how the information management system worked, they put it in the out tray and got it back in the intray, they didn't know the theory and practise behind that. We should not be making do that in digital systems either, it should be all under the water line, under the bonnet hidden away

We need to focus on our customers, embrace change, grow in how we deal with new tech logical thing because it's here to stay and we've seen a lot of it over the last 6,000 years. Otherwise I don't think we're going to be sustainable as a profession. That comes with being agile and flexible in the way we do things, moving away from rigid motions of what information and records management is to much more flexible outcomes and customer driven focus, and think about how we can do it making it easy for people under the water line as a service. But in order to do that we do have to collaborate with our partners in IT and we have to innovate in our own practice and our own academic backgrounds and epistemological thinking. We do have that deep underpinning of ethical practice. I think back 20 years to when I was doing my archives and records management masters about a third of the course was all about ethics. And I just don't see that replicated in IT professionals, I don't think they get that deep embedding of how information and data is embedded within the human experience and the human environment. They see it much more from the technological environment, but ultimate let reason we're all doing this is for human outcomes. If we're doing it for the machines, we're doing it for the wrong people. We see an awful lot of angst at the moment about the rise of the robots and AI. Well, is that partly an expression of how we've become disassociated from information and data, it's been a technological artifact instead of an expression of humanity

So I want to finish this off with a bit of positivity because I've been quite negative, how we're going to go the way of the dinosaurs. When it comes to dinosaurs they had a massive setback but ultimately they learned to fly and became the birds and they're doing all right for the most part.

That's what I want to talk about, to bring all of those concepts and ideas together about how we can evolve of our practice and evolve how we work. I see artificial intelligence and machine learning as a fantastic opportunity for records and information management professionals as much as any other profession. But I think it's profound for us because what it allows us to do is a lot of the things that we used to be able to do in the paper environment that we lost the control of in the technological environment for many different reasons. Organisations decided they didn't want corporate control of their

information in the 80s and 90s and they gave everybody a personal computer, the clues' in the claim it wasn't a corporate computer, it wasn't centralised terminal, it was personal computer, so we fractured and diffused information and data management down to the individual level and you still hear an organisation still whinging and moaning about how do we not have enterprise control, well, you've given everybody a personal computer around allowed them to do it differently so why do you expect a different outcome? Once you've given everybody individual control over this they expect individual control over their information, they don't want the barriers, or the perceived barriers and guardrails the standards and corporate control and ethics and all that stuff getting in the way of them doing their job, because over the last 20 years they've come to have the illusion that self-control of information and data is somehow more efficient and effective than having it done for you at scale.

I just don't think that's correct. I think what the rise of the internet in the last 20 years has shown us is that if you have systems that are standardised up the wazoo, automated, consistent, ethical and efficient, you get a much better experience with your data and information as a human. I use the example of the internet. You don't get anything much more standardised than that. You can use it on any device in any country in any language. The W3C standards and all the technical standards that sit behind it are rigidly enforced even to the point of the content itself. Google has cornered the market in that. If you don't set your metadata and your descriptive standards to the way work the Google search algorithms you don't exist, you don't come up in the searches and you don't exist.

Everyone has given up their control to the robots and to the overlords and the data masters already to get the convenience and the experience that we've now got with the internet. Who would go back 20 years to doing everything manually and having to go to the shops or the banks to do what they used to do. I am proposing a similar step change for how we work with our information and data and our organisations going back to centralised control, the efficiency of scale and the fact that we can start to do things like ethical considerations and standards and controls and getting good societal outcomes and taking away some of that risk at the edges, because it doesn't matter whether it's in the cloud or on prem, it's the quality and the controls and ethics around stuff that's really important. I would say the big scare around AI, what it's really showing up is not a new technology and a new way of doings things, what it's showing up is our pitiful data and information management, control and management within organisations. That's my contention.

Every time I've tried to do in the last 10 years or so working with government agencies, anything we've tried to do in service innovation or to make things different or better has bumped up against the same issue of data quality. It's not good enough. Most of the data scientists I've employed over the five, eight years have spent 50% of their time or more cleaning up data.

So for me we need to move to a world where we use ethical AI to identify strong use cases so we're not running away and giving up our control to the machines again, we do this as a considered corporate strategy and we do it as a government and we do it as agencies and we think about it and we don't rush off and just do things in the short-term to the previous point the long-term unintended consequences of fixing short-term problems could be an existential treat, with AI could be an existential threat to humanity.

I'm proposing with work with government to look at use case identification for machine learning and AI and a sustainable well thought through and ethical platform when we think about why we're doing it, what's it for, what the ethical considerations, what are the mātauranga Māori considerations, how do we do this where we can start safe and build up the confidence and the experience to start branching out to the difficult and fuzzy edges and don't start there.

So I guess that's my big pitch to the profession and to all of us in this room as public sector employees, is let's think about where we want to be in the next 10 or 15 years, let's harness this technology, let's get ahead of this technology, and let's use it and not be a victim and not be -- be proactive rather than reactive. If I think, when I was Archives New Zealand two years ago, I got innovation funding to work with Amazon and Microsoft, we did amazing work on the compliance of the service using machine learning and AI to get unstructured content to structure it, make it intelligence ready, put compliance into it, make it safe in an ethical way, we did amazing work, but no-one knew what the hell I was talking about two years ago.

But the time has come for it. Now people do know what large language models are, they do know what semantic and ontological understanding of content is and they do understand we've got to do this in an ethical way and it's game changer for all of us, but hopefully in a positive way. Thank you. **[Applause]**

How Can we Apply Digital Preservation Principles to Help Organisations be Digitally Resilient?

- **Joshua Ng, Carly Lenz**

>>Chris McDowall: Thank you Stephen. We unfortunately don't have time for questions for these two presentations but feel free to put them in Slido anyway for anyone to just think about. As someone who's working in data governance at the moment, the information team at MBIE are some of my favourite people to talk to.

Next up we've got Joshua Ng and Carly Lenz from Archives New Zealand and they are talking -- they're asking the question how can we apply digital preservation principles to help organisations be digitally resilient.

Josh and Carly are also administrators of -- they work as digital preservation analysts at archives and they're also administrators of the New Zealand government digital archive. They're responsible for the development of digital preservation policies and processes, file format, technical analysis, digital preservation system management, providing advice to government agencies regarding digital records management and born digital record transfer to Archives New Zealand. So please join me in welcoming Josh and Carly. **[Applause]**

>>Carly Lenz: Tēnā koutou katoa, ko Carla Lenz tāku ingoa. (Te reo Māori). Hi everyone here and hi everyone who is on the stream. My name is Carly Lenz, this is my colleague Joshua Ng, we are both digital preservation analysts over at Archives New Zealand (te reo Māori). You can hear my unfortunate American voice okay? Sweet.

We're thankful to be here at GOVIS today and to be talking to you all about one of our favourite things which is digital preservation. More affect lately known as digires within our small whānau and off the script, I'm just realising that digires could be the portmanteau for digital resilience if we want to normalise that a bit more, just some food for thought.

We believe that the principles at the heart of digires can increase digital resilience or digires at your organisations, that is the literal resilience of your high value information, the operational resilience of your information systems and subsequently the intellectual resilience of the memory of our government. That being said we have a short story to share with all of you. 100 years from now in a not so distant and hopefully cyber punk future humanity finds itself amidst global disaster. Another century gone, another pandemic on the doorstep, the more affected parts of the world grapple with the new reality of being a

hot bed for the virus. While others look on, waiting uncomfortably for the inevitable and waiting desperately for answers.

In one of these latter settings, we meet Meka, a public servant who has been urgently tasked with some fact finding. The brief to uncover information about the 2019 pandemic from the time, specifically regarding any governmental response, public health advice, or engagement on social media. The impending arrival of the pandemic in Meka's location has brought on an anxious atmosphere increasing the magnitude of this undertaking. He can only hope the right information is out there, that it's authentic and that it can be accessed.

While on Meka's quest for knowledge, he is faced with a vast information landscape, one full of unmanaged content, popular news and shine knee tools that spotlight current information, rather than the historical data that he's seeking. He's overwhelmed by what is out there and is beginning to feel unsure of the integrity and the relevance of the information he's finding along the way.

>>Joshua Ng: And so, Meka decides to take an alternate route and goes directly to a subterranean agency established during the time of the 2019 pandemic. This agency was small then and continues to be now. Operated by an equally paltry but enthusiastic team of information champions. The whole digital collections of vital relevance to Meka's [(inaudible)], but due to the agencies lack of resourcing the data has been stuck in a legacy system for ages and requires migration into a modern system for rendering.

At first Meka feels sadness, frustration, and disappointment, he thought he had reached a grail, the taonga that would provide clarity and act as a guiding light in the face of a modern global disaster. Old data kept in a legacy system, how could this be an authentic usable and accessible resource?

Upon expressing such exasperation the agency ensured while migration efforts were supported back in 2019, the information champions of yore had prepped a data environment for any potential future endeavours in the migration space. The integrity of the collection was unparalleled, file format identifications, related technical specifications, prominence notes, you name it, the elements necessary to enable integrity, usability and accessibility of this collection were present in the system and Meka knew that modern tools could not only unleash but also preserve the data for continued future keeping reference and use.

Feeling informed and empowered and equipped with a portable storage device, Meka left the agency his cup full, not only did he fulfil his mission but he was ready to return to his world with the desire to learn more about the act of digital preservation, the

activities that the agency undertook to ultimately ensure the auspiciousness of his quest. What could he share with his peers and organisation and what could be done now to set up digital resilience in the future?

The information team at agency had recommended assessment tools for Meka to explore. He was to bring them back to his organisation so that some internal evaluation could be done as a launch pad. One of these tools was the digital preservation coalitions rapid assessment model, DPCRAM, a tool developed back in 2019. Meka was told this assessment tool helps to measure where an organisation is at in regard to their digital preservation capability. The DPCRAM is purposely agnostic towards preservation strategy and solution, it also supports institution of various kinds by covering a broad range of digital preservation activities. Meka took note of this, planning to apply it to his own organisation.

>>Carly Lenz: Whilst rummaging around in the agency's holdings Meka had also come across a document from Archives NZ that diagrammed something called a digital preservation framework. Within this concept were different components, including principles, policies and outcome statements all working towards fulfilling an overarching vision. The principles stood out to him emphasising integrity and active management, particularly through a legislative lens. Meka wondered if the principles and the policies at his own institution focused on their digital holdings, or if they were due for review.

Armed with the right questions to ask, and the tools to measure their corresponding answers, Meka openly accepts the work yet to be done. There's more, don't worry, sorry, suspense, got to keep you in, right?

All of us here can be like Meka's helpers, we can be the information champions in the story. We might have set this tail 100 years into the future, but we although and understand that technological advancement, especially system migration, can happen in just a few years' time, and that we can confidently anticipate this progress. Many of us here have related stories of needing to deal with legacy files, either during a system migration or simply in our business as usual practice.

The Public Records Act specifically states that the disposal of information must be by the approval of Chief Archivist so legislatively we all have a responsibility to preserve our high value information. Of course in our current framework we at Archives New Zealand would welcome digital transfers.

Not exactly like this, the beavers -- not a problem for us at the moment and hopefully won't continue to be. But until then, until transfers are ready to come our way,

every agency represented here today maintains the responsibility to digitally preserve their respective information, to manage their records, to tend to their Bonsai. In this sense digital preservation is for everyone.

We the digital preservation team and the government digital archive administrators at Archives New Zealand encourage you to spark some introspection at our own agency, check out tools and refer to our guidance such as the digital preservation statement and the information and records management standard. You'll also find yourself on a valuable journey towards digital preservation and digital resilience.

There we go. Kia ora. **[Applause]**

>>**Chris McDowall**: I've got something for you here as well. Thank you very much Josh and Carly, I can see that you've taken your lesson from Brenda Ratcliffe there on applying the hero's journey to your presentation. Were they AI generated images? Yeah. Is it mid journey, yeah. Very nice.

1:15 - 1:45 pm: Oceania Stream: Digital Resilience in Papua New Guinea: A Judiciary Case Study

- **Grace Tamu, Cedric Robert, Mathew Ogai**

>> **Chris McDowall:** All right, next up, pardon me while I find my place on my paper. Last year we were fortunate to have some visitors from Papua New Guinea and I'm pleased to say this year we're welcoming back Grace Tamu and also her two colleagues Mathew Ogai and then joining us online from Papua New Guinea as well we have Cedric Robert. So Grace, Cedric and Mathew will be presenting on the theme of digital resilience in Papua New Guinea and providing a case study to describe the significance of digital resilience to the judiciary. Grace will be starting the presentation, Cedric will continue part way through online from PNG and finally Mathew will wrap it up. I'll just quickly introduce Grace, Cedric and Mathew in turn.

Grace Tamu is from Wabag district, she's been working in the public service and the IT sector for the last 17 years. She's a Cisco certified network administrator. After 14 years with the department of finance, Grace is now working with the PNG judiciary, national judicial staff services in the role of systems manager. She presented at GOVIS last year around is delighted to be back. Mathew is from Popondetta Oro Province Papua New Guinea he graduated with a degree in information systems and worked in the private sector for in our years, he's now working as an assistant network officer specialising in

voice network and switching across the judiciary network and finally set Rick is from Alotau Milne Bay province PNG, he's been working in the IT sector for three years since completing a diploma in ICT, he started off his career with the telecommunications provider Telecom and transferred to the PNG judiciary in 2021. He's now working as an IT support officer and is supporting approximately 1,000 users spread across the country. Just as you do.

So welcome up Grace who will be first.

>>Grace Tamu: [Applause] thank you Chris. Thank you GOVIS team. Kia ora, my name is Grace and I'm delighted to be here with my fellow colleague at the GOVIS conference in Wellington, beautiful Wellington to present on digital resilience in Papua New Guinea judiciary.

So a bit of information about my team and I. We all work for the judiciary in Papua New Guinea, the IT division, so my role is systems administrator, Mathew Ogai is our assistant network officer and Cedric, as Chris mentioned, is our IT support officer.

So here is our agendas. I will be giving -- I will start off with a brief introduction to Papua New Guinea, where all three of us come from, then I will move on to talk about systems resilience. After this, Cedric will present on user resilience, followed by Mathew finishing off with network resilience and how that's implemented in the judiciary.

So this here is a picture of our new quad complex. So for some of you who do not know where Papua New Guinea is, this slide shows our geographical location. So PNG lies 160 kilometres north of Australia and as you can see from the map, it lies northwest of New Zealand. So Port Moresby is the capital city, which is where my colleagues and I are based, and is approximately a 3 hours flight from Brisbane. So that should give you a fair idea of where we sit just above Australia.

So five fun facts about my country Papua New Guinea. One, PNG has more than 800 languages and approximately 1,000 different cultures, making PNG one of the most diverse countries in the world. PNG has a tropical climate and experiences two distinctive seasons, so we have just wet and dry season, unlike New Zealand with four seasons.

PNG is home to one of the world's only toxic birds in the world called the hooded pitohui. Its feathers contain one of the most potent toxins known to science. It looks cute but it's dangerous. PNG is home to the third largest rainforest in the world. So we are third in line after Amazon forest in Brazil and Congo. And the last one, PNG is situated on the Pacific ring of fire, thus we experience regular earthquakes, volcano eruptions and even tsunamis. So this concludes my brief introduction to PNG which I do hope you found

interesting and we shall move on to my talk on system resilience and its implementation within the judiciary.

So system resilience. What do we mean by that? IT systems resilience is the ability of an organisation to maintain acceptable service levels when there is a disruption of business operations, critical processes or IT eco-system. So simply put, it's the ability of an IT system to continue to function in the event of a disruption such as fault, disasters, cyber attacks etc.

So some examples of common disruptions in IT services back in the judiciary which we have experienced are power outages, system failures, both software and hardware, and unplanned network outages due to natural disasters.

So this picture here is of our data centre in the new court building.

Hyper converged infrastructure. So the judiciary's IT infrastructure is built on a hyper converged platform. So we have high grated all our systems if a converged infrastructure to a hyper converged infrastructure back in 2021, and since then this has greatly improved our systems resilience.

So in terms of resilience, a hyper converged platform has its benefits, such as it provides a single system where all hardware and software components are integrated, thereby reducing complexity, saves cost and provides faster scalability.

Additionally hyper converged infrastructure reduces the legacy risks associated with traditional architectures that require multiple components and improves IT agility where new services are easily and quickly provisioned.

Lastly, and I think most importantly, hyper converged infrastructure was built to provide high availability, which is a must have feature when your organisation is running a number of mission critical workloads, which is true in our case. So this feature has worked well for us in terms of having a resilient system.

So the judiciary has a hybrid infrastructure in terms of the location of our hosted applications. So with our current set up, 40 per cent of our business applications are hosted in our data centre on premise, while 60 per cent is hosted on cloud. So this set up has been quite resilient for us, as it provides high availability for our core business applications. For instance, when there is a long power outage, causing us to shut down our data centre, 60 per cent of our core applications is still accessible to internal and external users as it is hosted on the cloud. So you would need to just access those with internet data.

So that's the end of my talk. Ladies and gentlemen I would like to now introduce our next presenter who is Mr Cedric Robert who will be presenting online. So he is our IT

support officer. And he will be presenting on user resilience and its implementation in the judiciary. Thank you. **[Applause]**

>>Cedric Robert: Thank you Grace, good morning ladies and gentlemen. I am Cedric Robert and I work with the judiciary in Papua New Guinea as an IT support officer. My role in the judiciary is to monitor and maintain computers, basic network components, install hardware and software and solve technical issues as they arise. I will be presenting about the topic digital resilience which will cover storage back-up, business processes as the applications [(inaudible)].

Storage is one of the biggest challenges in the judiciary, how to keep data secure, reliable to access anywhere while having large (inaudible). Local back-up being the common storage method [(inaudible)] and the list goes on. It is a secure method, however once you lose a storage device you lose everything.

Network driver is a [(inaudible)] method. A storage device is usually created by a systems administrator having the data stored and accessed by the file server. The advantage of using the (inaudible) you're able to access your files using any computer or laptop as long as it is connected to the domain or through VPN access. (Inaudible) once the file server is down, everyone is not able to access and save their files. Microsoft One Drive is the preferred cloud-based application that we use to save files on as it is included in our Microsoft 365 licence. (Inaudible) we are able to access the files anywhere in the world on different platforms [(inaudible)].

The integrated case management system is the technology driven solution that has to be introduced in the year 2017 to the judiciary to (inaudible) and streamlined process for managing legal cases. So in the event when the IECMS is inaccessible or there is an internet issue, (inaudible) registry officers to file court documents.

So firstly [(inaudible)]. During that time this may be receiving a new (inaudible) or an existing one. When they ensure that the documents such as affidavits or statements of disputed facts and legal issues when government tried assigned and commissioned by both parties. Once they confirm they seal the document making it a legal document and a file number or reference number is generated manually.

Lastly, they scan the document keeping an electronic file record and the hard copy is sent to the filing room, that will go to the courtroom (inaudible) for hearing. For users who have laptops or wireless network interface [(inaudible)] which is satellite, or sometimes used [(inaudible)] during the time of network disruption.

Microsoft dynamics is the cloud-based application platform that our finance team use to do payments for vendors and suppliers. Whenever Microsoft dynamics cannot be accessed or when there is a problem arise with the external system the finance team [(inaudible)] develop a back up plan which involves manual bank. In the event an urgent payment must be made.

Here are some steps and processes taken to do payments. Firstly, they check the requisition with the correct approval and [(inaudible)] quotations. If a total amount is the same as the finance form, [(inaudible)] correct signatory. Once it's all done they create a batch and authorised banking. A cheque is raised once we receive receipt they confirm that we have done payment and the spreadsheet is created, marking goods and services as paid.

Lastly, [(inaudible)] advice is delivered to vendors suppliers, advising them we have (inaudible). Once the application is back online the respective officers will go back to the spreadsheet created and update the system as goods and services [(inaudible)]

For the Record is the application we use in the courtrooms to transcribe and record cases. The FTR system has an in-built (inaudible) that can last almost an hour when the power goes off. The application has four channels and saves audio with the tracks (inaudible) which is later uploaded to the share drive or the CRS server.

Thinking of a worst-case scenario in the event when FTR is inaccessible or the application (inaudible), there is a device called marans(?) which acts as a secondary back-up system, however, the device has one channel and saves files in the MP3 format. Later it is burned to a CD, taking a hard copy and a soft copy is stored on the hard drive as local back up, another [(inaudible)] is sent to the file server.

Another device which is on standby is the portable FTR system which is easy to set up and usually [(inaudible)] for court settings.

In the event when there is an issue, for instance power internet outage or other technical issue such as server being offline, we keep judges, external staff and external users through telephone being the fastest way to communicate from a very long distance. However, when the telephones are affected by the network, another way to advise users is through bulletin boards around different locations and dissemination of letters are hand-delivered to divisions. Informal communication is the most detailed way to advise users, explaining [(inaudible)] sometimes criticised by [(inaudible)] most times [(inaudible)] during the conversation.

Going back to my main points, I thank you all for listening. Now I will introduce the next presenter who is Mathew Ogai, our network officer. He monitors and [(inaudible)]

the network infrastructure across 21 sites in PNG ensuring all network components are functioning well. He will take you through the topic network resilience. Thank you

>>Mathew Ogai: Thank you Cedric. Good afternoon. Once again, my name is Mathew Ogai, I am the assistant network officer to the judiciary of Papua New Guinea. On a daily basis I assist the network administrator and show the network infrastructure across the country 24/7. In doing that we design configure and implement [(inaudible)] and wide area networks and research network technologies that will aid the delivery of justice to the people of Papua New Guinea.

In my presentation I will walk you through the network component we have in place and how the judiciary is managing resiliency within our network infrastructure.

The PNG judiciary has 21 sites across the country, they are connected back to Port Moresby over a primary connection which is the [(inaudible)] submarine fibre transmission which is operated by Telecom PNG. It is a state owned enterprise and operates telecommunication within Papua New Guinea. The judiciary has also deployed a satellite network as a secondary connection in the event we have issues with the primary connection, we fall back to the secondary connection.

This is a conception diagram of the PNG judiciary network infrastructure. The encircled is the headquarters located in Port Moresby, that house is our firewall which is mainly used for network monitoring, routing of internet traffic and also acts as a security perimeter. We then have the switching infrastructure that speeds up internal communication for judiciary staff between multiple divisions locally and remotely allowing (inaudible) to network resources. Judiciary has also rolled out the satellite network as I stated in my earlier slide.

As depicted, we have a fibre backhaul from the production to the disaster recovery site. In the event there is a system outage with the production site, we can fire up the disaster recovery site so maintain business continuity.

In terms of network security, we have an end point protection which is cloud-based that works together with the firewall. The end point protection identifies, prevents and takes the best course of action to isolate the PC from the network or quarantine the threats identified.

In regards to power we also have a genset that supports the whole judiciary when there is a power outage. But the IT department has also installed uninterrupted power supplies within the data centre to ensure there is a redundant power source into the data centre.

One of the main challenges that we are currently facing in Papua New Guinea is power outage. Power outage is a norm and it is undeniably and ongoing issue in PNG, so the PNG judiciary has taken several approaches in ensuring the network infra is safeguarded before power outage during and after power is restored. For the headquarters we have installed surge filters and surge protectors to safeguard our infrastructure in the event there is a power outage. Also in parallel we have an uninterrupted power supply, a primary and back up secondary power supply to ensure the network infrastructure is operational while awaiting the genset to kick in.

For remote sites, in order to maintain the delivery of justice, the IT department has issued [(inaudible)] SIM cards and smartphones with laptops to officers in charge of our remote sites, the ones in charge of the courts across PNG. So they normally do tethering with their smartphones to gain access back to cloud-based applications and especially our 365 email.

At the end of the day, ensuring the delivery of justice in a timely manner to the people of Papua New Guinea is paramount. So despite the approaches we have listed to address the power outage, at some point there will still be an element of failure present. So in cases where we have pour out ages in PNG, normally as far as three days without power the whole city goes offline. When that happens we normally fall-back to the traditional manual process as our second presenter highlighted where finance and [(inaudible)] division normally do payments to the bank manually, they normally go to the bank and stand in long queues to do payments with a cheque. Our court staff assist our lawyers, counsel to come to court to file their cases by manually scanning them and archiving them, then when the system comes back online they upload it back into the system.

So when that happens, the lengthy blackouts that normally happens, just for best practice the IT systems infrastructure team has to shut down the data centre to safeguard the infrastructure in case there's a spike in voltage or something. When that happens we go back to the manual process like I stated earlier.

So the judiciary is focused in moving into the digital space as a priority area, but as a developing nation there are challenges, overwhelming challenges we are facing right now. But nevertheless with logical reasoning and technical reviews driven by the benefits, the e-judiciary and IT team has rolled out several projects which are the [(inaudible)] network and satellite integration to all our 21 sites, which is 80 to 90 per cent complete now, which will enable us switching between our primary and secondary connection. Currently with

the infrastructure we have six internet service providers which we use in [(inaudible)] routing to do switching over if one fails based on latency (inaudible) and packet loss.

So one of the biggest developments -- can you move back to the main display screen please. One of the biggest developments in the region is the construction of the -- go back down again sorry. Can you move the [(inaudible)] please. One of the main big development NCSC the region is the construction of the Wabag court complex. It's supposed to come up. Sorry for the delay.

One of the biggest developments in the region is the construction of the Wabag national new court complex which roughly cost the judiciary approximately a billion kina. The monumental site comes with technical and systematic benefits which now we have three power sources into the data centre, so we have redundant, over-redundant over-redundant power source now. Hopefully that will assist the justice overcome power outage.

We also under plan is an appellate court system now. So we have a district court, national court, supreme court and the appellate court, but it is still under planning and review at the moment. And just for fun facts of the new building, we have eight different lift systems in one building. So projects that we are planning on embarking on, one of them is the digital bail. This will reduce the current over-crowding of correctional facilities, with the over-crowding of prison facilities it puts pressure on the staff and also a spike in the operational costs as well. So it will also offer the potential to reduce the number of detains in PNG correctional facilities by placing remedies and minor offenders under home detention

So we also have the judge's portal which is an information repository to assist judges, judge associates and village court officials in providing a centralised location and providing an ease to retrieve information. The application is a mobile ready application that allows judges and court officers to access it anyway just to have internet connection.

If we can move the slide down please, thank you. With the current projects and future projects that we are planning to embark on, is ultimately to deliver -- to assist us deliver a better justice to the people of Papua New Guinea. So with that said, thank you for the opportunity to share high level insights to resilience in Papua New Guinea based on a case study, the judiciary of Papua New Guinea. So please can you slide down the screen please. Please do not hesitate to email us, I believe there's a slide that will show our email address and contact details. Please do contact us via email or telephone us if you have some queries to ask, which I also believe you might have some information that would

definitely help us improve the delivery of justice to the people of Papua New Guinea. Thank you. **[Applause]**

Q&A: Digital Resilience in Papua New Guinea

>>Chris McDowall: We've still got a little bit of time before the next session. So if you've got any questions, feel free to put them in Slido now or put up your hand and we'll bring the mic over. But I've got one to start off with. And Cedric I'm sure is still listening in and can give us a ping on WhatsApp or something if he wants to answer too. But it was really cool seeing your network map I suppose of your ten regional sites and how you've got the submarine cable connection and the satellite back up. I was wondering are there any examples you can tell us a bit more about where the cables were broken or stopped working and you had to fall back on satellite and how did that work and how long was it until you could get the fibre connection restored?

>>Mathew Ogai: Thank you Tony. Thank you [(inaudible)]. Yes, it's a really good question. What actually did, last year we had an earthquake of approximately 7.4 magnitude in the highest region of Papua New Guinea. Our (inaudible) cable is, custodians of that cable is Datacom within Papua New Guinea. It comes from (inaudible) into Papua New Guinea. That cable was affected by the earthquake, it broke the express link out of PNG and also it broke the branches of that cable that connects other regions of Papua New Guinea as well.

So it was a really big disaster for us, so it was really good because we had the satellite redundant connection [(inaudible)]. So we had to push most, not most, but I would say all our priority users, Chief Justice, the executive management of the PNG judiciary out (inaudible). Basically they had access to only emails and web-based application so we had to disable graphics and YouTube access and all this just to free up the pipe so they would have faster accessibility, so that's what basically we did. So yeah.

>>Chris McDowall: Thank you, getting people off of YouTube, maybe that would be a challenge I don't know, got to do emails instead. We've had another question come through on Slido, so do you have issues with mobile network outages, do citizens use satellite connectivity as well and do you use Starlink or is it something else that you own?

>>Mathew Ogai: Thank you, I think there are several questions -- two questions. So for the mobile network, we roughly have four mobile carriers in PNG, Digicel, Telecom, Vodafone just came in recently. So with the mobile networks they have their own separate tower, so

most of the outage they're supported by their own power sources. So our mobile network I would say is redundant enough to sustain natural disasters.

>>Chris McDowall: Would that include cyclones?

>>Mathew Ogai: We have to have an experience with that to confirm whether it's resilient with a cyclone. For the satellite connection it's normally through organisations that have the financial capacity to instil the infrastructure. Unlike New Zealand, I passed by several stores I had WiFi access. It was really good and helpful with directions. But for PNG, our geographical location is quite inconvenient for us to have the infrastructure in place.

So like, for example, if I want to go to another remote site I'll have to hop on a plane, a 45 minute plane again to a remote site to do support work or to troubleshoot the network if there's an outage with our remote sites as well. So for satellite, it goes back again to funding capacity of each organisation, but it's not for the public to access and all that if you're asking.

>>Chris McDowall: I might just go to one last question. So the second one on the screen here, you've spoken a lot about infrastructure, but can you share a little bit how you iterate services in respond to changing needs?

>>Grace Tamu: Thank you Chris. Could you read the --

>>Chris McDowall: Yeah, so you've spoke answer lot about infrastructure, but could you talk more about how you iterate services in response to changing needs. So the people side, the culture, the process side, how do you show resilience in that way?

>>Grace Tamu: In terms of the services we provide in IT?

>>Chris McDowall: Yeah, all of the services you provide the judiciary, I suppose. When there is some sort of impact or problem, how do you -- I guess how do you let people know what's happening and what your response is, how do you, yeah, about communication and leadership and decision-making.

>>Grace Tamu: Okay. Thank you Chris. So I think one important thing that Cedric has mentioned when we do have our services are unavailable and we need to let our users know, communicate that to them, we go back to -- as Cedric mentioned we use our phones to advise the users, we also -- for example when the email is down as well, we put notices on -- within our organisation, we let our users know through notice boards and all. Am I answering -- yeah. What else.

>>Chris McDowall: If you're using the internet normally and that's not working, hour do you communicate and how do people know what to do. But I think you've kind of answered.

>>Grace Tamu: Also perhaps radio as well, that's one thing we could look at just to bring out the message that these are the systems that are down and, yeah, to advise the users.

>>Chris McDowall: We might be hearing more about this later in the afternoon, but it was, yeah, when cyclone Gabriel came to New Zealand mobile networks went down quite quickly because the battery back-ups ran out within a few hours in many places and all of the many fibre connections to that region of New Zealand, the Hawke's Bay, were cut, and so geographically New Zealand and Papua New Guinea have quite a few similarities, I guess we're island nation, we've got quite rugged topography, yours is even more, so earthquakes, volcanoes you name it, yeah. We'll wrap it up there, thank you very much for coming out again this year and speaking to us. If anyone has any questions or would like to know about digital resilience, these guys in their day jobs will probably need to display far more resilience for all sorts of things than any of us will, you can take it from them that's for sure. Thank you very much, Grace, Mathew and Cedric **[Applause]**.

1:50 - 2:20 pm: Oceania Stream: Lessons for Public Sector Reform from Australian Robodebt Royal Commission

- **Pia Andrews**

>>Chris McDowall: Technically we have a very short break between each presentation. So there's like a minute to go. I'll just use that time to turn the page. It's also a chance for you to discretely change rooms. Welcome back everybody, we're up for our third session in the first part of this afternoon. And coming up next we have Pia Andrews, who's on a, I guess a public service sabbatical, is that how you describe it? Her presentation is called lessons learned for public sector reform from the Australian Robodebt commission. And a little bit of information about Pia. She is an open government digital transformation and data geek who has been trying to make the world a better place for 20 years. She usually works within the public sector machine to transform public services, policies and culture through greater transparency, democratic engagement, citizen-centric design, open data, emerging technologies and real pragmatic actual innovation in the public sector and beyond.

She believes that tech culture has a huge role to play in achieving better policy planning outcomes, public engagement and a better public service all around. She is taking a public sector sabbatical and is working as a strategic advisor to the public sector and AWS. She has a newly formed team made up of experienced public servants who provide

futures orientated policy and outcomes focused advice, support, exploration and experimentation to agencies and departments across Australia, New Zealand and Oceania.

I'd also just like to say thanks very much Pia for your continued support for GOVIS and for our help with developing the program and many other things behind the scenes. Please join me in welcoming Pia. **[Applause]**

>>Pia Andrews: Being much shorter let's pull that right down there. Tēnā koutou, (te reo Māori) I'm very rusty, been away a year and a half sorry, but it's such a pleasure to be here today, thank you so much to the GOVIS committee and thank you all so much for coming to this session. I should quickly say I'm not representing my employer, I'm actually coming to you representing the Australian society of computers and the law with whom I did work to create a submission to the royal Robodebt Royal Commission. Because I know the public service here quite well because I know the public service in Australia quite well I'm something of a translator between the two and I know how big a deal this is going to be, not just now but in terms of massive reform and change across the whole of the Australian federal government and states and locals. I know it will come to affect you at some point, so I want to give you a friendly heads up.

So what I'm going to be doing today is going through what Robodebt was who, here has heard of it? A couple, not many, there you go, this is going to be traumatic for you. I'm going to tell you what it is, what was done, I'm going to tell you how the government has responded to date, and then I'm going to talk about the actual next steps and why it's going to have such an impact on a much broader series of structural and systemic reform that's happening across the Australian government right now which is very exciting and again useful for you to know about. I'll try to translate it into what it means to you as part of the process.

Robodebt. What is it? I'm going to talk through very quickly what happened. This is the shortest possible way I've been able to condense this down. So first of all it was a government policy back in 2015, 2013. What they wanted to do was to recoup $1 billion into the budget. That was actually the policy intention. Okay, I'm presenting this as a case study I'm going to give you all the facts and lots of references. The goal was just to get $1 billion back, there was no other policy intention no, other public outcome, they were just trying to figure out a billion bucks. They went around the departments and said find us a billion bucks. The MSD equivalent in Australia said very hopefully said boy have we got a deal for you Minister. They came up with some initial advice to their goal, their proposal

was that there was a lot of fraud in the system and they could probably get back that fraud from beneficiaries and that would probably equal about $1 billion magically.

So the initial advice on this proposal to recalculate previous debts -- sorry, previous benefits and then go after people who had been overpaid, the initial advice was that the method to do that, I think called income averaging, was not lawful, it would need legislative change, but they proceeded anyway

The next thing that happened there was a had he calculation of historical benefits with income averaging, just in brief, people in earn different amounts through throughout the year obviously, if you take one fortnight and use that to average out the whole year, you're inevitably going to get the wrong outcome, a miscalculation, as it were. But that's what was done, so they used a combination of data from taxation department, they did income averaging, came out with numbers, and then a very, very large number of debt notices were sent out over the next few years

Overpayments, in quotes because a lot of them were wrong, were framed as debts, and this is key. The onus of proof was reversed. It wasn't the onus on government to explain its decision, the onus of proof was actually on the recipient to explain hello such and such we paid you, we think it's wrong, we think the information you provided was wrong, you owe us $20,000 unless you can prove otherwise. You can imagine a lot of people, most vulnerable people, were traumatised by this.

So the debts were also just to really make it worse, outsourced to debt collectors, private commercial debt collectors. For a lot of people their phone number, their email, their physical address had changed in the last 10 years because some of these were ten years ago. Hey you owe us $20,000 from ten years ago but all the letters and correspondence to try and get people to engage on it weren't received. The first time a lot of people heard about the debt they owed was when a debt collector rang them, which is quite intimidating, or there was cases were people went to the doctors and suddenly the money wasn't in their account to pay for their kid it's doctors appointment because the money had been garnished. Really quite full on.

80 per cent, 567,000 debt notices went out. Of that, how many people here work in statistics or have a mathematical understanding? More of you surely have a basic mathematical -- anyway false positives in a good system should be Paddy in what sort of range? A few per cent, yes? All right, 80 per cent false negative. So 470,000 of those cases have been conceded to date as being wrong, fundamentally wrong, completely wrong.

Of course through this process and over the years this happened, dramatic increase in complaints, dramatic increase in people concerned, not just from people, but from staff, from tech, from people across the organisation itself. Some of those complaints resulted in lawsuits, some of them went to the Tribunal, some of them went to all kinds of different places but quite often people would settle out of court so fault wouldn't be found, there was some very interesting behaviours that have happened that all came through the Royal Commission

AA T the Tribunal found income average was unlawful and the person that found that was stood down from the Tribunal. The Ombudsman review recommended a review, very helpful. And it created sustained and extraordinary harm not just trauma and frustration and fear and intimidation and people not being able to pay for their kid's doctors, but deaths, there's about almost 2,000 recorded deaths that are associated with this.

So legal challenges were breached, so Australia's biggest civil lawsuit it, led to a settlement over 2020 and 2021 of 1.8 billion dollars which is obviously our biggest lawsuit, civil case. They also found again income averaging was unlawful. Very interesting.

The new government coming in which came in a year ago as part of their election campaign they campaigned on running a Royal Commission into this program into this scheme into Robodebt and that Royal Commission was conducted over the course of October December through until April or so this year.

The report that is being handed down in just a few weeks, I was hoping it would be handed down ahead of this presentation, but it actually got delayed so that it could be, my understanding so that it could be -- so that the adverse findings in it could be directly referred to the new national anti corruption commission which is being established in a few weeks time they wanted the report to be brought out after that commission was set up. Read into that what you will

So how was it reported on? How do people understand this? I've got a bunch of quotes up here, I'll send this stuff out but I want to read a couple of these allowed I think they're very interesting.

In 2020 the government conceded about 470,000, a false positive rate of 80 per cent from one of the universities as I mentioned. Robodebt should never again be framed as a technological glitch or a legal oversight, it was the active and direct exploitation of people's vulnerability from the conversation.

The justice responsible for the class action settlement Justice Bernard Murphy said it was a shameful chapter in the administration of the Commonwealth and a massive failure

of public administration. You can see this is a big deal for us and a big deal also for you, because as part of our session today in the safe house of Chatham House rule, we're going to be going through and doing some scenarios.

To this day I still get anxiety when I think about my Robodebt. The government should think about people who are struggling, people who have depression or money troubles, they should not put pressure on them and make their lives worse, from a recipient

One of the biggest surprises of the Royal Commission was just how easily many public servants, senior ones in particular as it turned out, accepted that Robodebt was legal and properly organised without basic checks and balances to affirm its legality before raising a legal demands for money.

And this is key, this actually came from one of the deputy secretaries inside the Department, she was amazing out of all of executives that gave evidence she was extraordinary and well worth watching particularly in contrast to some of the others. They had a strong view of the deserving and undeserving poor from the 2014 budget through to 2018, the vast majority of my work involved identifying savings options to cut social security spending

One of the things that came out of the Royal Commission is they interviewed a lot of public servants, a lot of frontline public servants, heads of departments, politicians, at least four including the ex-Prime Minister was called to evidence and that was fascinating to watch. But one of the things that really it did was it showed kind of the worst and the best of service. It showed some of the people who were like this is what the Minister wanted so we had to do it regardless, we provide the advice and they ignored it so we had to implement because they decided it which raises the question if you're asked to do something illegal do you do it just because the Minister says or is there something above the authority of the Minister which we'll get into

But it also showed the best, part of the evidence was given from frontline public servants from particular public servants from Serena Wilson from the people who tried to do the right thing, who saw it was not mathematically correct, who saw it couldn't possibly be legally correct, there was so much internal agitation to try to try stop change at the very least pause this scheme. So that was a very good thing from a from that perspective,

Would you mind right clicking whatever needs to be done there? No, it's mine, there we go thank you. Just one final quote, this actually was from the sub that, the Australian society of computers and law did, the Robodebt scheme has exposed significant cultural structural and political issues in how public institution have administered and

managed public policy. These issues compounded by how technology has been misused. This is key. A lot of people look at Robodebt, it's a great story of the dangers of automation. You can have terrible designed policy, designed systems, but if you've got the right culture measures monitors feedback loops even terrible systems can become good. Even good systems that as the environment around them changes can respond and adapt to those. This is really a story about how we are structured to be, to the theme of the conference, more resilient to change and more responsive to change.

There's a great quote by our current Prime Minister if we don't shape the future the future will shape us. We've been looking at a lot of risks and AI how are we going to react to AI, but it's more about how do we get to the future state that we try to get to, how do we fulfil our [(inaudible)] purpose and leverage these things in the right way in the context and special needs and special accountabilities of government.

What's been done then? Obviously there was the AAT findings and Ombudsman reviews. They have ceased the program, settlements of course and the Royal Commission. But they also, this is key, they ceased the outsourcing of debt collection. They recognised maybe that wasn't cool. And there has been a major program about re-instituting the core capabilities and competencies of the public sector which is quite exciting. The royal report's coming down, the adverse findings, but there's also a major, major -- this is one of the things I think will be helpful for you potentially -- reform around policy practice and policy capability, and how policy actually operates end-to-end. There is a significant understanding that set and forget policy is not working.

So let's look at the current policy experience. You've got the policy team sell grating another great job, we got it out the door now on to the next policy. In the back of the mind, I wonder if we could raise different ideas, where these ideas come from, I wish I could see it through, but no, on to the next thing. So the policy instructions go into the black hole of policy intended. Yes, I made all this up but roll with it. So from this black hole of policy intent and purpose comes the instruction, the delivery team, might be from legislation a team inside a government, might be legislation of a regulated entity, any idea what this means no. They've moved on to the next thing, let's do our best. That creates an impact and the people affected by bad policy, it can literally ruin their life this black hole of policy impact, you have no idea what the impact is. No-one's monitoring for the ongoing human, environmental, other community impacts, they're monitoring for whether they're meeting their policy intention at best and evaluations tend to look at the same thing.

Eventually time passes and the evaluation team talks about why was there low policy impact and real harm from the start, they should have evaluated sooner, but evaluation is a point in time. So we have a really broken policy cycle, policy journey. And the gap between policy and delivery is huge and of course it's also not traditional. The gap between policy and delivery was brought in only 25, 30 years ago with new public management.

Prior to that you had a social worker writing social policy, prior to that you had an outcome with all the capabilities needed to deliver the outcome. There's lessons from the past we've lost that we could get back into. And I won't jump too much in this because I do want to get in the table workshop. What time does this go to? 20 past

Let's talk about failure. So my observation? We had a failure of public service mission purpose values and culture clearly when what you're doing is completely contradictory to all that but you still do it there's a systemic problem there. There's a failure of lawful and responsible administration, clearly. There's a failure of accountability, because even though all those mechanisms for accountability did their reports and found they were doing the wrong thing it didn't change anything. How can our accountability mechanisms actually drive change, not years later. Failure of independent review there were independent reviews from a number of different companies but all of those reports were effectively kept in draft and never actually actioned. In fact one of them didn't actually end up fulfilling their report at all they ended up doing a PowerPoint slide. Failure to understand and mitigate unintended impacts, no escalation mechanism for staff. If your chain of command ignores what you're saying, the only other option is whistleblowing which everyone is afraid of. How else can you report and get something changed. Failure in policy design clearly but also failure in policy responsiveness and a duty of care. Also in political neutrality

Basically I've been trying to help senior executives across the public service in Australia to remember what the minister says is only in the middle. Legislation in our constitution sits above that in terms of authority, departmental policy and implementation planning sits below that to a degree, but the idea that you only have a mandate if the Minister says it or you can't do something unless the minister says it is just not Westminster

The impact of Robodebt on the whole of government in Australia, is obviously driving a shift in policy capability and policy practice, driving a shift in workforce training and public sector craft and everyone having to be taught maybe we shunt do that because it's illegal it's driving a shift in out the executive layer is trained, how they're rated in terms

of performance which is fascinating, shift in culture, shift in accountability and responsibility very interesting, driving shifts in actual policy not just technical policies like AI, digital data etc, workforce management but also driving a shift to how social policy will happen for some time to come

And it's actively feeding into and creating demand for the APS reform agenda. So very briefly the APS reform agenda which you have no reason to know about, it's the exciting thing in the world right now, quick quote.

There is work to be done in repairing years of neglect suffered by our public institutions. Outsourcing, poor resourcing clunky systems and a decade of deliberate devaluing of the APS has meant the Australian people are look at our institutions with a jaundiced eye. (Reads).

I don't know how much all of that sounds familiar, but the fact that the government of the day is acknowledging that as a problem to solve is quite exciting. The APS reform agenda is going -- not just digital or service reform it's actually about structural, cultural, purpose reform. So trying to build an APS that embodies integrity in everything it does, that puts people in business at the centre of policy and services, not just services, you can have citizen-centric services but if you don't have citizen-centric policy you're always the tail wagging the dog.

And APS, it's a model employer and that has the capability to do its job well. The amount of policy teams that outsource policy development to the private sector is not good, but whole chunks of core capabilities have been just eroded over many years, so that's a real challenge they're trying to fix.

And why is it going to happen this time because we've had reform agendas before and the simple answer is pressure. Not just Robodebt Royal Commission, Covid demonstrated the problem, we have a massive integrity review called the Coldrake review, the challenge and opportunities of AI is driving a demand for change and of course expectation change more broadly.

So couple of key lessons then we're going to do a table exercise briefly. First of all public servants are responsible for lawful responsible implementation not just good advice. Not just good advice. Frank and fearless advice has become a bit of a barrier to good administration, because the perspective so long as I provided good advice, if they chose the wrong decision that's not my fault. Well, responsible implementation, stewardship of long-term public good is part of it. So the APS reform agenda is instituting a purpose statement in the public service act in Australia for the first time ever. We are a penal

colony. Our public service was set up as a punitive measure now it's learning how to be set up for the good of the public which is good

It's also setting up stewardship as one of our core public service values, not just about reacting to the government of the day about long-term stewardship of public good which is really cool.

And of course the voice will be a really amazing opportunity for that as well. The onus of proof is on government for government decisions not on the public, which is a basic premise of the Ministry of law, here in New Zealand you have section 23 of the OIA about a right to an explanation so that should be a core business requirement and principle for all of your business systems.

Evidence-based and test driven policy, could identify issues early of course. Sometimes up need to say no to the Minister of the day, is actually one of the key lessons, monitoring for policy and human impacts is critical to mitigate harm if you're only measure for policy. It was technically successful it did bring a lot of money back in from a policy objectives perspective it was successful but just because it's meeting objectives doesn't mean it's achieving the right outcome

Model needs to be reformed. Feedback loops are critical, don't outsource core government functions, not just policy but debt recovery, don't create unexplainable untestable and (inaudible) decision making in government and public servants are more than just administrators, we have to be stewards of public good. So even if something legal doesn't make it right and that line is one that we need to tread.

So just quickly, this is what's happening in Australia, people are realising just that's been that way doesn't mean it has to be that way. There's a real shift, everyone below the senior executives feels vindicated from the Commission because they saw their own, the frontline people, the tech people, the lawyers even who were like this is wrong, and the general public like we need to recreate this sector in the vision of these people, that's such a vindication, these speech have been trod on for so long

Whole bunch of links in this slide deck I'll send out, but what we're going to do is have just quick table thing, rather than Q&A I'm not the authority of source of this, just wanted to raise it, I want to do a little exercise with you. If everyone could cluster around a couple of days so you get more than one or two people at a table. While you do that I'll quickly quote something from the Minister for APS reform at its heart this is about restoring the public's trust and faith in government and its institutions which I think is quite wonderful. I was going to do two exercises but we only have time for one. I'm going to

use this one. I want you to think about your department, where you work, and I want you to have a conversation, have a kōrero about using the Robodebt scenario, if it was you working in that department and given that instruction and being told to implement it, I want you to have a genuine conversation about what are the escalation mechanisms available to you in your context that would help you actually remediate or mitigate the harm that would help you inform a change of the policy, that would help you avoid the absolute disaster that we have had not just for the public service but more importantly for the people. Because here's the thing if you can use Robodebt as a scenario as part of your planning and thinking, then you might be able to avoid the awfulness we've just gone through. That's my little challenge to you

Have a conversation, I'm not asking for a specific outcome, you don't have to report to the room, this is all Chatham House rule, have a think about how could you say no, in the face of political pressure, what mechanisms exist to you, how would you mitigate this scenario in your context in your situation, please have a chat and then we'll get back together in about five minutes. (Conversation). I'll just grab your attention back to the front please. Now I made you to write down your answers with names and departments -- no. So mope three hopefully that's been a stimulating conversation. The goal here was not to say here ears the answers, the goal was to tell you about this thing that's happened and to encourage this conversation, the conversation you've just been having

My suggestion is that GOVIS, we have nothing like GOVIS in Australia, I'm trying to set something up because it's such a wonderful model but it's a safe community of public servants. My suggestion would be if this is something you think would be helpful email the GOVIS committee and suggest a few sessions where you could have the conversations and build them out a bit as a community. But I hope that's been helpful, I hope that's been useful and thought-provoking and please do keep an eye out and set a date in your calendars for 7 July which is a day -- it's either the day or day after the Robodebt Royal Commission review is being handed down the report, because it will be very interesting reading, and for those who didn't know about it before, sorry, for those that did hopefully it's fleshed it out a little bit. In any case I do hope that some of the lessons that either that I've shared or you yourselves will draw will be helpful in helping you to leapfrog and to help renew and do your own level of reform to make sure you are being the best public service that you can be as well. So thank you all so much for your time, have a really great day, really appreciate it. **[Applause]**

2:25 - 2:55 pm: Oceania Stream: Digital Resilience Lessons Learned from Disasters

- **Simon Mason, Fiona Dally**
- **Chair: Mike Chapman**

>>Chris McDowall: Excellent, coming up in just a few minutes we have a panel discussion here in the Oceania stream so we're just going to set up for that and we'll be ready to go in a few minutes I expect. **[Pause]**

>>Paddy Power: Okay, I think we'll kick off this session. So now we have a panel on digital resilience lessons from disasters. So we've had -- I'm just going to wrangling the Slido questions, you can put questions into Slido as we have been doing all day. If you're online put questions into Slido and vote them up. And I'm going to hand over to Mike Chapman who's our chair so introduce himself and the panel. Over to you Mike.

>>Mike Chapman: Thank you Paddy. Kia ora tātou. My name's Mike Chapman, I am the manager systems strategy and standards at Archives New Zealand. In a previous life I also worked for the Ministry of Civil Defence which is why I was nobbled, I think, to chair this group to keep these two honest on the panel. Joining me to talk about lessons from disasters are Simon Mason from census collection operations for DCE in stats, and Fiona Dally, lead advisor national security system MBIE.

What we will do is go to each of the panel members and give them a few minutes to introduce themselves in a bit more depth and also a brief overview of any emergencies they've been involved in, I use the term emergencies there specifically, slash disasters slash catastrophes slash unplanned events. They all apply and the response should be the same. And how they dealt with it.

>>Fiona Dally: Kia ora, thanks for the introduction mic. In terms of MBIE as you can imagine it's quite a broad Ministry that covers lots of different aspects in regards to events and incidents. In terms of my role, I act as a conduit between MBIE and the ODESC system in terms of when there's a nationally significant event and the system is activated. So it means a lot of herding cats and coordinating from across different business groups within MBIE to provide that one source of truth out to our chief execs and out to that broader ODESC system when it's activated.

In terms of the types of events that I've been involved in, I've been in the role quite new, only a couple of years, but as you can imagine, Covid-19 was a huge coordinated response from within the Ministry and I was part of that. Also more recently was in the

national crisis management centre as a liaison officer for MBIE supporting the national emergency management's agency response to cyclone Gabrielle and the Auckland floods, and the probably less visible ones that were also concurrent this year, I led the all of government coordination around the carbon dioxide supply shortage, which also began end of December last year, and have also been involved in some of the visa immigration processing responses.

That's a quick introduction on the types of events I'm involved in. I don't know if it's useful to pause and you do an introduction then we talk to each or mic, do you want me to talk to how MBIE's dealt with them?

>>Mike Chapman: There's too many to talk about them all, which maybe the plague of envy in its size and the issues you have. Was there a common theme?

>>Fiona Dally: Perhaps a good one to focus in on is cyclone Gabrielle and also, for me, what does digital resilience look like. Again I'd like to make a big plug for business continuity planning, it's not necessarily something I've heard a lot of visible talk of today, but again it's about what prior arrangements have agencies got and their data centres and third party suppliers that have planned in advance for when things go wrong, so that we don't have to respond in such a reactive way and we have prior arrangements in place. So that for me is a big piece, particularly from an all of government business procurement perspective that we need to focus on in that critical prioritisation of services.

For MBIE we had quite a specific frontline role in the Gabriel response in regards to temporary accommodation services, rapid building assessments, setting up visa categories specific to the recovery. Key them at ix as always is timeliness and urgency of these things, in a disaster the challenges and opportunities around how we data share and have -- the need to have good baseline data quality that we can access in times of urgency, and certainly that's key themes that have been carried over from Covid in terms of how we need to work on those MOUs to strengthen the links between local government and central government agencies in regards to data sharing.

One that we might not think of but is also very simple, MBIE is the fuel sector coordinating entity. In times of the cyclone people need fuel to get their generation working, to get the digital capability back, and again, we are looking at how we can improve and have that real-time GIS system set up so that retailers and agencies can see which fuel outlets are actually open or closed and how we can support that real practical things that people need to know when there's limitations on communications or urgency

around timely information. But that's just some of the top line things that come across our desks.

>>Mike Chapman: Yeah, one interesting point there that you were involved in both parts of was the Covid-19 issue, as we all were, but that led to immigration issues. So you sort of had an event upon an event related but never ending.

>>Fiona Dally: Absolutely. I think, the theme that most agencies are seeing is the rise of concurrent events, and the reality of that fatigue management piece with quite a lot of people working on multiple responses, so this is a plug for people who are interested in helping to get trained up in that coordinated incident management system, it's really important that we get people who don't necessarily see themselves in that response sector to consider the skill sets that they may be able to offer into incident management and support in response time, because we certainly do need to work on that common operating picture of the datasets and the value of those are invaluable to communities and decision-makers.

>>Mike Chapman: I'd like to pick up, we'll move into the census area. But with the theme that I picked up from yours around the people too and the effect particularly as we were talking outside, the effect of cyclone Gabrielle on the census takers. You may wish to give a broader background to it, but yeah, that resonated.

>>Simon Mason: Thanks mic. Tēnā tātou katoa. Ko Simon Mason ahau, I'm the deputy for census, that guy. Responsible for 5 million people filling in a form either online or in person.

So is everybody familiar with the word pivot? Yeah. We pivoted a lot. Starting with Covid we were scheduled to run some major tests to help us with census and work out what was going to work and what wasn't going to work. Covid came in and locked down almost all areas that we were going to test in and we had to pivot. That meant we didn't get to test everything we wanted to do. That started us off on the back foot and meant that some of the systems, some of those digital systems that we rely on, we didn't know if they were going to work, we didn't know to what extent that they would work, and that caused us a bit of grief in the operational period.

Then February came around and storms blew in and Hurricanes arrived as well, and we had to pivot again. We had to pivot quite majorly in the East Coast of New Zealand as Fiona started to talk about, where the social good of doing a census where people should be worried about digging their houses out of all the awful sludge that they were stuck in became the focus and burdening them with a census and another piece of paper wasn't the right thing to do. So we had to delay that by several weeks while we also went in and got

money from cabinet to help us extend the collection period. Probably to the point where I suspect the Minister of Finance has me on a dirty black list where I'm now not allowed to ask for any money.

That cost us $30 million, that extension. Again, we had to pivot in terms of some of our operational approach when we did go back into the East Coast of New Zealand. I was up there both during the -- slightly after the cyclone and most recently a couple of weeks ago where the team was telling me they had to hire horses and boats and they had to hire jet skis in order to get the census out to where it needed to be. And the interesting thing about these major disasters is they almost always occur around a census. Now I don't know if there's a correlation there, certainly not my doing.

But we have learned that we need to be responsive and reactive to the community. So when the community says don't come, we don't come. When the community says we are now ready, then you can kind of go in. Because we want people to have somewhat of a positive experience when engaging with government.

But we worked quite closely with NEMA and Civil Defence and all those other agencies that supported the community during the cyclone event to get census message out there, to get the census out there, because the census is ultimately vital to how you build a community because it's the major source of how we calculate funding in this country. So it was vital that we didn't not do it, or did it in a time that suits for the community. The response rate was slightly lower for the East Coast, but we spent a lot of time trying to build rapport rather than doing something to a community.

So in terms of how that manifested into digital resilience, shortly after the cyclone we helicoptered in some of our people with StarNet to stand up local community hubs where they could not just do the census but where they could go and communicate with the world, because the communications were extremely poor, probably all read about it, cellular reception didn't work, radios were scarce and people felt devoid of communication for a large period ever time

So we pivoted a lot in terms of how we delivered the census during that particular event. So that's some of the story

>>Mike Chapman: Thanks Simon. I think some of the message I'm trying to get through is there was a digital resilience requirement, digital response, but it actually relied on people. It relied on the individuals, it relied on those people that had had just come out of Covid and we've all experienced Covid fatigue, sick to death of the bloody thing, and chuck in a

cyclone, flooding, not sure what we book for next week, but it's ongoing and it comes back to public servants to respond to those things in a variety of different ways.

The concept of sending in census takers to ride around on horseback actually has some appeal, personally it would be different from sitting in an office or God help me in the basement of the beehive and I have been there before and that's a horrible place.

It's versatility and it's building our strengths. One of the questions we'd sort of identified here was the information that you'd come out with, the disasters you'd responded to. Has anything changed in your systems now and looking into the future, your operating models that have, as a result of cyclone Gabrielle, or one of the many that you've dealt with, Fiona?

>>Simon Mason: Might just go very quickly, so stats does a collection operations for a number of different non-census surveys. We have field collectors out seven days a week most of the year. So one of the things that we've had to react to is environmental event and those ones a decade storms are now coming once every two years and in some places almost annually. So we're having to constantly pivot to get people to be aware of the situations before they go out into something that they're not able to cope with. Because these are just becoming more and more regular event. So that's changed our operating model to be more diverse rather than centralising in particular parts of the country to draw in responses. We've become a lot more reliant in other parts of New Zealand to represent parts of New Zealand that we can't get into due to these weather events.

>>Fiona Dally: Certainly a couple of areas from MBIE's perspective. Really the strength of that enabling local and regional business support aspect goes without saying that's a major component about how MBIE enables funding through to the right routes for distribution into the communities.

Specifically there are opportunities to strengthen the mandate that organisations like LINZ have, I think there's a couple of colleagues that may be in the conference in terms of that geospatial data and having really strong prior arrangements in place for both New Zealand-based but also international based geospatial data that becomes really important in the research and response aspect. I know there's been a couple of good wins in the budget bid in terms of improving data for the impacts around climate change and mitigation and also the New Zealand coast lines and looking to the future around all data capturing that needs to be done.

As I mentioned in the on the ground in terms of business building assessments, getting prior arrangements in place with the local authority so the data sharing and transfer

can be smoother in times of response is certainly something MBIE is focused on improving as part of lessons identified from this event as well.

>>Simon Mason: Sorry mic can I just add to that. I want to change my answer to what Fiona said as well. The data is becoming really much more important and we're finding also as an agency people want -- are willing to suffer the quality of, lower quality of data in order to get some data in order to make decisions so that's becoming vastly more important. So our organisation usually aspires for perfection, so 90 per cent quality of data, and we've had to lower that quality in order to get some of the information out there in order to make decisions. So that's becoming a shift as well.

>>Fiona Dally: Inc also a very obvious point but one that's worth saying from a more systematic perspective the early warning systems. Sorry Paddy, time to be quiet. Getting the message hurry up. Any ways, NEMA and working with the scientists to ensure we maximise technology and data to that 30 seconds to 1 minute difference can actually make a fundamental difference to saving life. So it's really exploring how we can improve and build on that capability as a country as well.

Q&A: Digital Resilience Lessons from Disasters

>>Paddy Power: Sorry, I didn't mean to interrupt you, but that's how it worked out. So we have got some questions coming through on Slido and we've got 10 minutes left so I think it's time to go on to the questions if that's okay mic. So the first one we've got here is how do you persuade people to invest in business continuity planning, it can seem like a waste of time?

>>Fiona Dally: This goes back to the fundamentals across for us in terms of risk reduction and readiness, from my perspective and to I think some of the conversations that were in the risk scape discussion, the $1 spent now on mitigation versus how much, $15 saved down the line, it is about both life saving and money saving. So to have those robust plans in place is going to help, there is a whole lot less pain down the line. It does concern me from an all of government perspective we don't have that clear critical prioritisation around when Wellington goes down what's the top five services that need to be delivered to maintain payment systems, Datacom, who's prioritised etc. So whilst it may sound a bit boring, it is fundamentally important for one these big catastrophic events will come along and be on such a bigger scale than what we have just unfortunately been through.

>>Mike Chapman: I think also it's been seen as very time-consuming, and the effort for return. It shouldn't take much time as all now. We've had plenty of practice over the last 3 or 4

years in business continuity. It should be dead ease tea to sit down one afternoon and bash out a continuity plan with the experience we've all achieved. I've got my tongue in my cheek when I say that, but it should be easier.

>>Paddy Power: Next question is, how do you stop people going into hero mode during a disaster and burning themselves out?

>>Simon Mason: Build more heroes, it is a good question because it does happen all too often when you rely and build on single points of dependency in these types of events. Usually it's the first person to pick up the mantle and lead on an those people get tired very quickly.

During the cyclone we had a regimented process where we made people take leave and return to their places of -- usual places of residence outside the situation so they could take leave because they were actually no good to anybody if they burnt themselves out, least of all themselves. So that's just one of the things that we looked at.

>>Fiona Dally: Yeah, certainly from an MBIE perspective we're really focused on that breadthening the bench and that capability and capacity building may be the least likely people that might actually really enjoy getting into coordinated incident management and targeting them for the specific functions, but I think it's really important that welfare and wellness management and people are at the heart of any response, so has to be really integrated into the check-ins and the people-centred focus to make sure that people can't get into that situation where they're 24/7 for 12 weeks of a response.

>>Paddy Power: So we've got another question, we've got lots of questions here, the top rated one at the moment is what does Stats NZ's thinking on how to digitally transform to be resilient in the face of these disasters?

>>Simon Mason: At the moment a lot of our input comes from face-to-face, certainly for social outputs that we produce. We're actually embarking on a transformation where we will shift to more administrative sources of data. So what that means for us is that we need to help government agencies build their administrative sources into statistical sources which means the quality fundamentally may need to change. That might take years for some of those sources of information, and some of those sources of information may need to be created. Again, that may take years. So we are actually already thinking about how do we transform ourselves over a multi- year period to get to a more resilient status where we're not relying on more human face-to-face contact which is not only waning on the public who don't want to answer their doors anymore, and they don't want to see somebody come and knock on their door and ask them a whole bunch of questions and take two hours in their home which is what happens at the moment.

>>Paddy Power: So there's a comment, this isn't really a question but a comment, and you might want to respond to it or you might not. True digital resilient would mean it wouldn't cost millions to pivot. No, I didn't write that.

>>Simon Mason: I can't put a cost to -- would it take -- does it take millions? I don't know. In terms of our experience, it has taken millions to extend the census because it's such a large scale activity, it's the largest peace time activity we do in this nation. So it costs a lot of money in the way that we do it. What we need to do is change the way that we do it and that's one thing we're going to talk to the public of New Zealand over between now and maybe next year around what does future censuses and those sorts of things look like. And hopefully lower that cost. Nobody's going to tell anybody are they?

>>Fiona Dally: In terms of that digital resilience, I think, a quick shout out to the telecoms sectors, there's obviously a lot of great work going on and that opportunity for users to access more in the future, I'll not name companies, but in terms of the ability to have New Zealand wide connectivity is going to be great in the future. Also, again, plug that critical dependency piece. An isolated resilience strategy is only ever going to be as good as your critical national infrastructure resilience and/or your disaster risk resiliency. So, yeah, less silos more collaboration is always going to be a good thing to save money.

>>Mike Chapman: Agreed. But what resilience do we have for a solar flare?

>>Paddy Power: We've got a few more questions in Slido. Is there anybody in the audience with a burning question that they can't be bothered typing in? No? Okay. I'll ask -- what frameworks -- I think we've already covered this but the question is what frameworks do you use to manage disaster response, how do you keep on top of everything. I think this is the Sims thing you're talking about.

>>Fiona Dally: I'm trying not to have an acronym central day, so thank you for those who have commented in the frame here. The Sim structure is a multi-agency response-wide recognised approach to coordinated incident management in New Zealand. There will be a review and 4th edition next year, but for now the 3rd edition is it. And the whole idea it's scalable, it's agile, it can be adapted for your needs and I do truly believe that it's been very useful for us.

>>Mike Chapman: I think actually it's the core response to anything effectively, from road smash to major earthquake, in that it works.

>>Paddy Power: The last question we have is, is there value in having the head offices of government departments distributed over regional offices, what might this look like?

>>Fiona Dally: Again this comes back to good business continuity and broader that piece about flexibility by default, and to build resiliency by not having all your IP as in your intellectual people and property in one place. So I think it should be something all agencies are considering in terms of the distribution of people brain people and assets, as I say that's going to be fundamental when unfortunately we have a major catastrophe and we need the default arrangement from Auckland to stand up. So the more people that work outside of Wellington now the better.

>>Paddy Power: Okay I think that's -- that's all we have time for. It's time for our afternoon tea. I'd just like to thank mic and Simon and fee own April for that discussion, I think that was really interesting and we have got some small gifts for you, which I'll give to you in a minute, and if you can all express your appreciation in the usual way. **[Applause]**. We're back here at 3.30.

2:55 - 3:30 pm: Afternoon Tea

3:30 - 3:35 pm: Ice Breaker Activity

>>Chris McDowall: That's almost a consensus there. It's great to see the ambition in the room. There's still 2 minutes left before we kick off with this next activity. I'm just going to, it being the afternoon and everything, it's easy to sort of run out of energy, so we're doing an icebreaker activity which we tried with all of you last year, all those at the conference. It's basically a rock paper scissors knock-out tournament. You're all going to have to get up and pair off with somebody, play rake paper scissors, make it the best of 3 if you want, but sudden death or best of true. If you're out please go and stand on the edge of the room and the remaining people will pair off and compete against each other, I can confirm there's a prize for the overall winner so please take this very seriously, thank you. (Rock paper scissors comp).

All the people sitting down, I'm going to assume that you have lost and you're out unless you're up on your feet finding someone else to go against. Who's still left? I'm out. We need to have our final in the middle of the room somewhere, it needs to be a big deal. Who's still up, put your hand up please? Sorry, who's still in. We've got three, we've got two semi-finals then a final. I don't care which one, who goes against who. Okay, that looks good.

All right, we've got Stephen from the gov team program as one of our finalists and Fiona from MBIE is next finalist. Here we go, a round of applause. Am I right, Stephen, if you're in it you're the finalists and you need to have it out. Come up here and do it please. I'll get the prize ready while you do that. Actually I should be a sports commentator instead. Here we go, I'll count to 3 and on 3, choose your rock paper or scissors, 1, 2 -- all right, 1, 2 -- just start, you have to do it yourselves, I can't do it. Fiona's won, congratulations. **[Applause]**

3:30 - 4:10 pm: The Chiefs Talk Digital Resilience

- **Mark Horgan, Bill Moses, Suzanne Pullman**
- **Chair: Richard Foy**

>>Finn Russell: Good afternoon, welcome back to the Oceania room for our afternoon session. My name is Finn Russell I'm a member of the GOVIS committee, outside of that I'm business an list at the Commerce Commission. I very much appreciate the opportunity to present this session of the conference. As a relatively new public servant -- excuse me, we have some great presentations coming up so thank you for sticking around. We have two presentations left today, which will take us through to the end of the conference and the networking drinks, so that's very exciting. Our first presentation is a panel discussion. The Chiefs talk digital resilience. Thank you tore Don Christie and Catalyst for sponsoring this discussion.

We have lined up several chief officers from the throughout the public sector to discuss the views on digital resilience, both personally and in terms of government organisations. They'll be discussing the big risks that threaten our public sector organisations and how they see us strengthening our resilience to mitigate these risks. So I'll just introduce everyone. Our first panellist is Bill Moses Chief Information Officer for the Public Service Commission. **[Applause]**

Bill has 10 years of government experience and more in the private sector delivering large scale digital government projects. Bill's work and his passion centre on linking people, organisations and projects together.

Secondly, we have Suzanne Pullman, Chief Information Officer at the Commerce Commission and funnily enough my boss. Suzanne has 13 years of IT experience in government including three as CIO at the Commission. Stepping up just weeks before the

global Covid pandemic emerged. The challenges that the pandemic exposed intensify the priority of digital resilience and set this domain as a key focus area in Suzanne's role.

Our final panellist is Mark Horgan, the chief advisor to the CDO CIO at the Ministry of Education. Mark has a background covering teaching, representing the government's trade with China, consulting internationally in knowledge management and working in various strategy focused roles including with the government Chief Digital Officer.

Finally the Chair for this panel is Richard Foy, a former Chief Archivist at Archives New Zealand. Richard is a tech-savvy futurist who is enthusiastically committed to leadership in and the prosperity of the public service. Over his career and within his personal life, Richard has embraced the cultural diversity throughout New Zealand and has been successful in leading effectively throughout his professional life.

So without further ado, I'll hand over to Richard to begin the chief's discussion on digital resilience.

>>Richard Foy: Okay, thank you everyone, thank you for those kind words Finn. Ngā mihi, ki a koutou katoa. Ko Richard foyer Ho. I'm Richard Foy, it's a real pleasure to be here this afternoon near the end of the day of GOVIS which has been a fantastic day, I hope everyone's had a great time.

I want to, in particular, at the end of this day thank Katherine who's right at the back who's been doing a fantastic job of transcription. And she's now having to transcribe her own name in the record. I had a talk with Katherine before, because it's really quite fascinating to see how she's doing this. Using a little transcription scene stenographer gang etc and a whole bunch of skill. We were talking about how some of the words she's transcribed have come up with some quite interesting transcriptions. I did ask, I said to her I'm going to call-out some of these, they're on us ladies and gentlemen, because if we don't speak slowly and if we don't enunciate, then she can't transcribe them. It's not her fault, okay?

So some of the really funny ones I wrote down before, sound pretty innocuous, that was wazoo, I think it was Stephen Clarke that mention the wazoo, that came out as wa sue, so that's pretty okay. There was malware, that became mall ware, what do you wear to the mall. Copying, that was cop peeing, that was a funny one wasn't it Katherine. Then of course ticketing which came dick etching. If I'm -- yeah, that's perfect, fantastic. All right. So that's just a bit of a laugh. We've got, hopefully a great panel this afternoon, three chiefs, Mark is a chief advisor, that's why he's allowed to sit here, so that's fantastic.

I want to, I guess I want to start by asking, have any of you learned anything today or heard or seen anything that's changed your sense or conception of what we mean by digital resilience. I'm going to use that portmanteau of digires. Did you learn something?

>>Bill Moses: Kia ora Richard tēnā kōrua Suzanne and Mark. (Pepeha). Thank you everybody, I'm Bill, I'm the Chief Digital Officer at (te reo Māori), what have I learned today? We'll go back to the first talk from NCSC. I think a lot of us here think our agencies are quite nice and secure, we hope they're all quite nice and secure, but I actually went to the NCSC website, I'm going to have a look at the framework and just double-check, that's the first thing I want to do when I get back to the office on Monday.

>>Mark Horgan: Mark Horgan tōku ingoa, just from that same session, I was absolutely staggered that for one of the most sophisticated frameworks around malware, or mall wear, passwords, at a very, very basic level, will practically eliminate that risk. Not completely of course.

>>Suzanne Pullman: I was going to suggest the first session as well. I went to the, not public digital cloud but the cloud project one and there were two things I came out of that one. One is that we're getting a replacement for the cloud 105 questions which I cannot wait for personally. I think the other side of it both on that conversation and the other one around cloud was that there is still such a big conversation around cloud and sovereignty and there's no right answer yet, it's just a conversation we need to keep having.

>>Richard Foy: Suzanne, when you turn up to work on Monday, because I would imagine you're going to go to work on Monday, and Finn comes up to you, he won't do this of course because he likes his job, but imagine one of your team come up to you and they say this GOVIS thing you went to the other day on Friday, what exactly is digital resilience? Because I mentioned someone I was coming to a conference and they asked what it is about, and I said digital resilience, they rolled their eyes, I can't blame them, what are you going to say to them?

>>Suzanne Pullman: I can understand that, resilience is about what you do to strengthen and prepare, whether yourself or your environment and how you're ready to bounce back if something does happen, and whether that's digital or any other area of resilience, that's in a nutshell what it means to me. So it's nothing crazy, just preparing, being strong at the beginning and bouncing back if anything does happen.

>>Richard Foy: I like what you said about in terms of it's about systems, you also mentioned ourselves, we'll come back to that one a bit later. Mark or bill, anything to add to that from your own definitions or readings?

>>Mark Horgan: Certainly the culture side of this is probably the most important. I think in terms of we know that the risks that are exploited, I don't know, I can't remember what the number was quoted today, but I think it was around about 80 per cent of the incidents had human interaction. So if we're not making sure that all of our staff and contractors and everyone else working in the organisations take security seriously, then our digital resilience no matter what we do in terms of cloud services and whatever else, we're screwed basically.

>>Richard Foy: That got transcribed correctly mark, screwed, absolutely.

>>Bill Moses: I'm going to take this quite slowly just in case. So totally agree with Sue Suzanne, so given the title of our chiefs talk, digital resilience, agree with Suzanne, so there's a personal aspect to resilience and I think the word pivot was used by stats earlier in a talk and being able to prepare yourself for changes that come. But in terms of our organisations, it's our responsibility to make sure our organisations are prepared for digital changes that come. AI is jumping up on us at the moment, so we need to make sure the organisation is prepared.

If I could put a system level perspective on that as well, given where I work, it's ensuring that all of us know that we can actually work together to make the public service resilient in the future. So we did quite a bit of this after lockdown to make sure that we shared a lot of our security protocols, settings, change management processes, making sure that we could all be prepared for the cloud, especially those of us who had already been through that journey, how we can support those of us that were you in to the journey or part way through the journey and give them that kind of collateral so it would accelerate their digital maturity. So got personal, our own organisation, and if we as public servants think about the system as well that would be good.

>>Richard Foy: That may be a good segue into a question I had around what the system is doing at your level as chiefs to have a conversation about resilience and actually building that resilience into the system at multiple levels. Bill you've said kind of what's happened because of Covid. Is there something ongoing that's happening and who's talking to who?

>>Bill Moses: I'll start. There are probably some projects I'm aware of, obviously aren't given some of the Slido questions. Let's think about where we work. So we're in Wellington at the moment, I'm assuming most here are from Wellington hands up if you've journeyed to Wellington to come to GOVIS today? Welcome. There's a project going on at the moment for regional hubs around the motu. So if you think as a public servant you should be able to work wherever you're needed and you should be able to travel and pop into a public service

office, open your laptop and connect. So that's a project we're working on at the moment, it will start with a central building probably bone house which is the building being renovated opposite the beehive. Will be a building that any public service can come in and use. We're working on the protocols and standards for that at the moment, but that's the premise or the vision for that building. If we get that right, maybe we can have centralised credentials for public servants as well. Maybe we can have ubiquitous WiFi around all buildings in the public service so you should be able to go where you want, access whatever you want, might even be a government public servant directory good forbid.

>>Richard Foy: Mark and Suzanne what do you guys think of that.

>>Mark Horgan: With the Ministry of Education we have dual responsibilities, one is for the organisation and the other government agencies. But the one that we've been focusing on considerably, and some of you might have seen a presentation by a couple of colleagues here around equal digital operating service, and the real resilience we need across the nation is for every whānau in the country to have internet connectivity, ubiquitous connectivity if we're going to do things digitally. We found that we needed to respond during Covid, especially, we've been doing it beforehand on a smaller scale, but Covid gave us the reason to say to government this is an issue, and it needs to be funded, which they've done now for three years, we recently got some funding to extend it through to an odd time in schools, middle of the calendar year. But this is something that needs to be an all of government service in terms of not just digital resiliency, but resiliency for every whānau to be able to operate in New Zealand.

>>Richard Foy: You're thinking about resilience of communities as well.

>>Mark Horgan: Absolutely.

>>Richard Foy: Not just infrastructure. Fantastic. Suzanne, Commerce Commission.

>>Suzanne Pullman: Yeah, I'll stick to a smaller system. The Commerce Commission doesn't have a lot of public facing digital interactions, so we do have a website and we do have certain things with industries we regulate. But that means a lot of my job and my team's job is the resiliency of the Commission ourselves. So our staff members and our systems is a little bit insular looking.

A lot of what we're doing is around that and the training of our staff and treating the wider resiliency. As a simple example on a practical level we posted something recently to all of our staff around do they know how visible their information is online, do they know what's actually being shared on linked in and other sites, how can they protect their information and that side of it. I do know that some of our branches though are looking at

resiliency, if we think of one of our regulated industries is fibre. There's a lot around what happened with cyclone Gabrielle is there more they can do to ensure the strength of those networks and the strength of what's happening. Not what we quite get to look at, ours is a little bit more about what we do to support the Commission themselves to then do their job, but that's being thought about.

>>Richard Foy: Could I get you guys to be a little bit vulnerable, obviously do this in a safe way because you don't want to expose your threats and vulnerabilities and weaknesses. Can you identify one or two things that you feel are the most vulnerable things you do need to work on in terms of resilience within your organisations today and actually are you guys having conversations not just with yourselves and your teams, but also with the executives? Who wants to start.

>>Suzanne Pullman: I can grab this one. Touched on it a little bit before, butter it is and always will be your people, no matter what you think you have trained people in and educated them in, you will always get caught out. And this morning the NCSC talk, he mentioned that they provide incident management response and I actually tried to catch him to thank him because we had an incident ourselves, it didn't go any further, it was stopped because of the protection we had in place, but a staff member still fell for a phishing attempt, we thought we'd trained them well and they didn't quite catch it. So learning who to target within the Commission and who to really focus training on because they might be our frontline for emails, or you know, your executive assistants get all the emails on behalf of people that will be attempted to be scams or phishing. So that's an area we just continually try and educate and do further in.

On a systems side of things resilience for us, we still have an on premise server room at the Commission, so actually on premise, it's on the same floor I work on which is crazy. On it is our document management system. So that is a big area for me, I think it's still -- we need to do something about it and what does it look like to move that. But that is a scary thing because you go okay, do we stick with the system, are we changing what we look at, there's at we behemoth of Microsoft, do we just go to sharepoint online, that's the next big thing for us.

>>Richard Foy: Old school Suzanne, on premise. You can go and touch and go all our data is there.

>>Suzanne Pullman: It is quite good doing show and tell every once in a while, this is what a server room looks like.

>>Richard Foy: As we had in the conversation this morning maybe that's the right scale you need, so interesting, okay. Mark or bill? Can you say mark.

>>Mark Horgan: From within the organisation, I'd say exactly the same, around staff education. I can't remember who the quote is from but the price of freedom is eternal vigilance certainly is something to keep going ahead. But we also have a responsibility for 8,000 early learning centres and kohanga reo, 2,500 schools and kura, and around 8,000, although that came down a little bit about Te Kupenga tertiary institutions. And we say in the compulsory education sector, which is the schooling and kura, that we have 2,500 CIOs. They all make independent decisions about the services and things that they run for their organisation. But some of them are extremely small. A principal and one teacher or maybe just a principal who is the teacher, through to 2,000 staff, depending on the institution.

We need to support their capability, we do that partly in the compulsory sector through a crown company called network for learning, and in the tertiary sector through the research and education advanced network New Zealand. They have some gross security mechanisms to help, but it always comes down to people in those organisations who will be targeted. Schools have their data frozen on a regular basis through malware, and are not necessarily able to recreate that.

So as small businesses, they get crippled. So we'll always come down to people, we can put in a number of systems and processes to mitigate those, or lower the risk, but it will come down to people.

>>Richard Foy: Bill, Public Service Commission, what do you guys do that -- sorry, I'm not asking what you guys do, but what are the things you guys worry about? Because you are actually quite different than both education and the Commerce Commission.

>>Bill Moses: We get involved in everything Richard, mostly a policy answer. But I think what do I worry about, what Mr Hughes worries about. But from an organisational point of view it's fear of the unknown when our deputy chief Melitsa and I go to the governance board we've just got to -- we don't know what they're scared of so we've got to tackle that. Melitsa will be running an awareness program over the year so we encourage people to share their digital experiences and remove the phobia around digital and data so they're open to the conversation and new things that are coming up, that would help us out a lot.

>>Richard Foy: Do you guys have any questions for each other while we're here, I'll just take a moment from what you've been hearing? Or do you think some of your colleagues should be thinking about some other problems that they haven't mentioned?

>>Bill Moses: Okay, project that is really dear to my heart is fed rating across the public service. So when I think about the public service, obviously given my role that's what we generally do, we're thinking about the public service, Peter doesn't necessarily care too much about the Public Service Commission but he cares a hell of a lot about the public service and he cares about every one of you.

So when I think about that, thinking about how we can federate with each other, how we can join up with each other, what are the easy, low hanging fruit that we can all just go out and pick and implement, and you're all technology or data in the room, you should all be talking to each other and sharing your skills and experiences and seeing what you can do individually to make things better.

Don't wait for your system leads to run a project. Don't wait for GCDO, bless them, don't wait for GC DS, don't wait for cyber-security, if you see something needs happening go and talk to your peers and your community groups and do something about it, get them all together, share experiences and just make it happen.

>>Richard Foy: That's leadership ladies and gentlemen because I was going to say isn't that the role of GCDO & GCDS.

>>Bill Moses: They are there to support you they will 100 per cent back you, but there's a lot to do and they have a limited number of resources to do that work in. So they're relying on all of us to get together to do this stuff.

>>Richard Foy: I want to ask you guys how you keep abreast of all the problems of the world when it comes to this notion of resilience, and we've talked a little bit about systems and processes and people, actually I might mention what came to my mind I think Suzanne when you talk about people, if I think about Radio New Zealand they have a system that involves a lot of people as well as tech knowledge and they had a break-down in that system which eroded their reputation recently.

That wasn't an external threat it was an internal threat. Is that something that you guys think about much or have to deal with and how you're thinking about these things. Is it just when some execs come up with some we're scared about this because we saw it on Radio New Zealand news, or are you guys systematically caring about this. Any thoughts?

>>Mark Horgan: Systematically caring about this absolutely. Insider threat is -- in government as much as it is in private enterprise or anything else. And we take a liberal view of that, so it's not the look at everything to check that everything is happening, but certainly periodically logs are looked at. I remember some time ago and happens regularly just to see what search terms are being used and what material is coming through our filtering

systems etc. And if something's found then we'll certainly look into it. But it's not something that we take a big brother view, but certainly that insider threat is always there.

>>Suzanne Pullman: If I may be talk to more of the keeping abreast to what's happening in that space, we -- a big thing for us is connecting into the NCSC alerts which were mentioned again but just general tech news. You're going to find out about anything being exploited pretty quickly in that space as well. We've done a lot of work internally around vulnerability management and putting something that's scanning our networks and checking regularly but that's one side of it because it can do all of the scanning but if you don't have a team that's on top of it that wants to do something about it and actively makes the changes it's not going to do so either, so culture change. We've shifted a lot to not having the security people being the ones making the actions and the decisions on what to do, but it's a conversation between our security and our engineers, we're seeing these vulnerabilities, what's the most important thing, the next step and how do we work through it. So big culture changes there.

Something Bill said earlier reminded me as well, when we think about the big scary things of what our execs are doing, a little story that happened with us, myself and a general manager got an email saying hey we've got a huge risk on our registrar from our board, there's this huge risk around chat GPT and the risk was that we're now going to get bombarded with fake submissions because of chat GPT.

It was this funny moment of they had no clue that could have happened for any time, you just copy paste, do it think other way but they'd heard chat GPT in the news and wanted a big risk front and certainty on the register about it. So it was a good responsibility to educate and go yeah, that is a risk but not that big and not new it's been there a long time and talk through how it doesn't matter too much, that's not the biggest thing for us. That's the other thing as well, keying in with the crazy conversations and sanity coming into it.

>>Richard Foy: Anything to add to that bill? Little stories, that was a great little story that one, love it.

>>Bill Moses: I can't shut up. Just the point to carrying about the communities to practise, working in with them, making sure you're sharing in your learning bank as well. I think there was an analogy I heard today which is you join a Facebook group and you really engage with the Facebook group and you might be putting up posts and everybody else comments on it, as you mature in that Facebook group you stop putting out those posts and you start commenting on those posts and eventually you're reading those posts thinking

OMG the same question is coming through. But we're at multiple phases of our career, going from the younger to the older, so we need to be there to support each other.

I think stories when Suzanne and I worked together we brought in some, in terms of learning, brought in some high school students to come in and do I think it was work experience, it was a couple of them that came in and they were really excited, quite energised to come in and see what real adults did.

So we sat them down at a desk and put them in front of a computer in a screen and we introduced them to some other people and they got to experience the day. How did it go? They said do you sit at your desk all day? Well yeah, yeah. What things do you think we should change? We just look at our phone and the phone signs us in, so we're thinking okay, hello service would be quite good. But learning from the next generation is something that you want to do on a regular basis. Our intern at the moment has introduced us to a new term which is all G. You'll have to learn that from an intern

>>Richard Foy: Okay, like all good, not all GPT 4.0. Okay, talking about younger generation my daughter's trying to ring me right now and I've been hitting cancel three times, she's very resilient.

I've just got one question to ask before we go to the Slido boards. We've talked about resilience, about building in capability, capacity, dealing with crisis events. What about the people, the human element that sits behind our ability to run these systems to look after infrastructure, and how to I guess build in resilience about people. I'm not talking about technical capability here, I'm talking about the ability to turn up to work, make sense of what's going on, follow, lead, and get on with things. Is this is something I care about a lot having gone through my own lack of resilience recently. What are you doing for your people because it's not getting any easier, right, adapting to change is getting harder and these crisis events are getting more complex. Any thoughts folks?

>>Mark Horgan: We certainly found, I'm sure this is the case for almost every organisation following lockdowns, was that there was a huge variety in how our staff and our management reacted to the idea of coming back into the office. Some from health reasons were averse to being in there in close, so as you know we all had distancing between desks etc, etc. That's continued for some people who still remain anxious about that.

There were others who, having been away from physical interaction with people, wanted to be in the office all the time. And we still running, I don't know, about 20 per cent, 25 per cent occupancy I would say. It's really quite low.

What I have noticed in some staff have had to reach out quite strongly to get them, meet them and then bring them back into the office because their resiliency was lower by not having that level of connection. So somehow connection, certainly with teams and Zoom and all those things, you can have quite a significant level of connection. But there are some of those things where the physical proximity is something.

So there's a -- your question's very deep and there are many, many aspects to how do we think about resiliency in a human space.

>>Richard Foy: Thank you mark. Suzanne?

>>Suzanne Pullman: Yeah, I think a big thing is the culture you create and the culture you foster within your teams as well. So work/life balance is incredibly important to me. I don't think you can be resilient at work if you're already expected to deliver 100 per cent every day and then when some crisis comes in you don't have any extra capacity to do anything else as well. If you're already at 100 per cent where does that next thing fit in. So I really want to foster and build a culture, I think we're quite successful with this looking at Finn is our team being People First and caring about each other first and knowing that life is a lot more than just the hours you're at work. That's a huge thing. We've had a -- we've had some hard experiences at work. For a smallish commission we've had five people pass away in the Commission in the last four years and you come away from that as a team remembering how important life is and building together stronger in that team as well. So I think that's part of it, and that's the biggest part of it for me is that culture we build and supporting each other. Yeah.

>>Richard Foy: Yeah, okay. **[Applause]** bill, anything from your side.

>>Bill Moses: Just to go after Suzanne, we run a service arm, IT as a service arm, like the people facing element of a service arm, so if I'm showing my vulnerable side I really struggle with work from home. So in terms of individuals asking if they can work from home we stopped that from happening and we stopped it from being my decision and we made it a team decision. So that was an aspect of me trying to pivot and change and dealing with my insecurities around working from home and making it a team agreement that we had working from home. And in that aspect I think we are sitting at 60 per cent occupancy day-to-day apart from Tuesdays when we're all in the office. We're trying to do that in terms of leading the organisation and making an example.

Q&A: The Chiefs talk Digital Resilience

>>Richard Foy: Thank you, thanks for talking to that. I think we'll go to the boards, Slido. There's one question I can answer, which is Richard Foy what is your rank in Starfleet -- I'm a captain, that's that one done. Here's one for you Bill, can we have a public sector office in Auckland too? Not too sure that's your decision.

>>Bill Moses: There's two of them up there. So hands up if you're from MBIE. Whether or not you know this, you're in charge of the Auckland policy office, so the Auckland policy office actually it was set up for policy people to travel to Auckland and just use the office. So you've technically got one up there already but that's being renovated and reinvigorated. There's also a building being stood up in Manukau referred to as the Manukau hub, so the dirt hasn't started being dug on that one but the plan is starting for that.

>>Richard Foy: I'll just go through some of these from the top. This question, is there any reason you or we invest in proprietary software over open source? This feels like a resilience issue. Is it?

>>Bill Moses: Might be some examples required. Are you referring to Microsoft technologies there? They're mostly based around open frameworks, I imagine there's two or three architects around here that could answer that question better than I could. AAD for example I know is based on an open framework. We can integrate those types of things with open frameworks if you need to.

>>Mark Horgan: We have a whole plethora of services run on open source software. We do run quite a bit of proprietary software as well that's quite true, depends on the need and answer to the RFP that we put out for the various things.

>>Suzanne Pullman: It's an interesting one, I think as a smaller agency we will stick to some of the tried and true and knowns as there's a lower cost of entry because you know others are using it and it will pass the security side of it as well so there's less risk associated with choosing something that's more of the proprietary that others have used. It's a funny one I've been thinking about, the Commerce Commission part of our role is around monopolies and fair competition in the market yet you'll choose Microsoft for word and outlook because it's the right choice, it's funny we've been thinking about it as well, how we making sure we're sticking to our own rules of competition.

>>Richard Foy: Not simple answers are they, they have wide-ranging implications because of the collaborative nature of the public service, which is a good way to connect to this next question, which is further to bill saying agencies need to work together, how do we actually

do this about with so many barriers with sharing, for example dollars, access, and how do we not re-invent the wheel? Have you guys got any thoughts on that?

>>Bill Moses: Why did you pass to me?

>>Richard Foy: It's not just on Bill.

>>Bill Moses: It's not just on me, it's an answer that we all have to create. So I'm going to point to Melitsa again, we ransom workshops with public servants to say if there were no boundaries physical or digital to your collaborating working together what would you do. We weren't asking for a technology response from them, what would be enabled if we did X, Y and Z, and we got some really good answers back.

I think the most practical responses we got were from people leads, HR leads across the public service and the digital leads across the public service, we had some good feedback from them. We asked the new professionals network to come in and talk as well. They were the ones that -- there was only two things they really wanted one was access to people's calendars and public service directory. Sometimes they're simple things we can do.

One of the things I'm trying to do at the moment, admittedly it's a hub and spoke model, federated teams access across the public service. So education are open federated, but for the rest of you, I think I'm up to 30 agencies at the moment, which allow for free chatting over Teams, so long as your agency federates to the Public Service Commission. Eventually we'll all be open federated, we can all freely chat with each other. Those are simple things that we can do.

>>Richard Foy: I think we're getting to the end of our time. There's only one -- I'm just going to ask one question, probably one of the philosophical ones, see what you think. This is will humans always be the weakest link for digital resiliency? You can just go yes no maybe. What do you think? With are we actually the weakest link?

>>Suzanne Pullman: I'm going to choose a cheesy answer, I think we are the weakest and the strongest link, I know it's a cheesy answer but it really is.

>>Richard Foy: I know we need to move on because there are people following us. So big hand to Suzanne, mark and Bill. Thank you.

>>Finn Russell: We have a little gift for each of you to say thank you very much for your time and your insights. **[Applause]**. Cool, so on to the next presentation.

4:10 - 4:45 pm: Cyber Security in a Broken World

- **Steve Honiss, Elf Eldridge**

>>Finn Russell: Our final presentation is titled cyber-security in a broken world and comes to us from Elf Eldridge and Steve Honis from ZX Security. They'll be discussing the necessity of organisational resilience towards cyber attacks, and a pragmatic approach to security based on the realities of attacking and defending organisations with disparate digital infrastructure and staff.

A little bit -- do you guys want to introduce yourselves? Cool all-righty, so without further ado, here is Steve and Elf. **[Applause]**

>>Steve Honiss: Hi everyone, Steve Honis, I'm the director of cyber strategy and risk and ZX security. I look after the governance risk and compliance team at ZX. I guess 50% of our business, our clients are government accounts of one sort or another. Everything from central agencies out to local government. So pretty familiar with working in this space and for my sins I spent 27 years working in government itself before moving into security because I needed to escape and do something different but I ended up consulting back into government. So that's me, Elf.

>>Elf Eldridge: Kia ora everyone, I'm Elf from ZX, I'm part of the penetration testing team, so when I'm not here I'm breaking into your systems and stealing things I shouldn't. And I guess the interesting thing from the last question are humans the weakest link, just to jump back on that for a moment. That kind of implies that computers aren't and I would beg to differ. My day job is breaking into things that aren't supposed to be broken into and they're pretty bad. I find if harder to scan people than I do to break into machines. Humans aren't perfect but computers aren't either, let's make that really clear.

Shall we jump in and do some slidey things. We did the introduction of ourselves and there's a photo of me trying too be more interesting than I actually am. Steve I think we have your stuff first.

>>Steve Honiss: Yeah, I thought we'd kick off having a chat about governance. It's a potentially boring topic, but it's super important in the space of information security. And for those people who are practitioners it can make life a whole lot easier if you're working in a place where governance is a thing and it's working well, and for those of you who are in leadership roles it's really important to understand what your role is in digital leadership and particularly as that relates to security.

The Institute of Directors have put out some really useful information, it's up on the website, that gives some good guidance on governance in the security space. In recent years we've seen much more attention being focused to security by boards and sort of flowing down from that to E L Ts, S L Ts and so on with the key point really being the outcome or the realisation that security isn't just the IT department's problem to care about, people have got skin in the game much further up the food chain than the IT ops manager, and we're starting to see that a lot more now across both boards I'm working with and other clients that we're working for as well. So what we expect I suppose is that we'll continue to see that increasing realisation or appreciation of the importance of good governance in security space.

The point that the IRD make about cyber risk needing to have the attention of the top table is a really important one, and there's a couple of ways that will get influenced, both externally by influencing the directors themselves, or themselves becoming aware or educating themselves about the importance of it, but also by pushing risk up, escalating risk up the hierarchy so it gets the proper attention and decisions around resourcing to deal with risk can be taken at the right level in the agency or the company as it may be.

One thing that we regularly talk to clients about is the importance of having cyber risk on the agenda at all of those ELT meetings and board meetings, as some of you are likely from crown agencies where there are boards in place, others won't have them, but whatever the peak body is within the agency that you're with, that's where cyber risk needs to be discussed and I guess pleasingly it is certainly amongst our customer set, we're starting to see that a whole lot more now which makes a big difference. Boards are well used to and ELTs are used to considering health and safety, that's been on their radar fairly and squarely for quite some time now and it's taken really, really seriously. So balancing up other risks to the organisation is starting to become more common, but super important.

One thing that we like to see is the natural tension too between the management layer and the ultimate decision-makers, whether that be a board or whoever else around accepting risk. Often we'll have, whether it's through penetration testing or assessments that my team do, identify some pretty serious risks in an organisation, and on occasions we'll have IT managers or CIOs saying that's terrible, we better not tell anybody about this. Which is the worst thing in the world, right. The decision there is getting taken by somebody who probably shouldn't be making that decision on behalf of the organisation and really doing everyone a disservice including themselves. By escalating that risk up further to people who can make decisions on it, that's where the risks need to be considered.

And we've seen some really good outcomes when that does happen. Boards don't like to have the wool pulled over their eyes, CEOs don't like to have the wool pulled over their eyes and when they do and something goes wrong that's when it can get really sticky for people who have been involved in the decision-making.

The place where is we've seen the best success and getting resourcing and attention paid to security is where risk are, escalated, the spotlight's shone on them and they've been pushed up high enough where decision-makers get to say well either I'm comfortable with that risk which is a perfectly fine outcome as long as that person who's making the call on it is the right person to make that decision or they'll decide no, I'm not comfortable with that so then they get to make a decision about funding or resourcing, the remediation or tidying things up.

One thing that we've found really useful is the use of a risk framework or a controlled framework for assessing and managing and tracking progress and using security maturity. There's a couple of ones on the side there, the NIST cyber-security framework which is the one with the five circles or the five components around the outside and the other is ISO 27001 which is a pretty well-known one. We often use NIST because it's applicable in any environment and the five functions aren't the outside are easily understood at a macro-level, but underneath those they boil down into 23 categories and then I think it's 108 or something like that subcategories that are quite granular controls that can be used by operational people for implementing new controls into an environment what it enables you to do is measure maturity against that, it means you can see return on investment, progress over time, as a security program's being undertaken

This is an exam number a slide deck that I use with one of the clients of mine. This goes up to the board every quarter to see progress against each of those five functions over time. And the board don't want to see much more than this. They want to know the progress that's happening. If anything stalls or if there's any particular issues, then they want to know about that so they can make some decisions about it. But otherwise as long as though lines are tracking up they're happy because they know things are heading in the right direction. So I'd really encourage people who are working in security space or I guess if IT more generally if you're not using a framework to track progress and maturity then really have a think about this, do an assessment from the outset and you can set a path forward.

Some really key questions that we often get asked by board members, what do I need to know? What are the things I should be asking my management folk about. And

these are some examples of them. But really it starts with what do we need to protect and that's people understanding their business, what are the critical assets, information assets that they've got, what are the crown jewels, what would cause a really, really bad day at the office if it got compromised. And unless you've had a good think about that and started to work backwards, then you're kind of on a high end to nothing. If you know what those key assets are you can start to make decisions flowing on from that

Understanding what your threat profile's like as well, or the threat profile against you, whether you're a big or small target. Elf will talk about targeted and opportunistic attacks as well, understanding who might be interested in you and how big a profile you have. The questions around business risk that I've talked about already, but really critically look at where those decisions about managing those risks are getting taken if it's getting -- if high risks are being accepted at an operational level, then there's something not quite right. So probably a rethink around that needs to be taken.

One question I always encourage boards to think about is whether they've got the right expertise on the board to be able to consider information security risk or cyber risk. They've generally got somebody who's got a legal background and somebody who's got a finance background of some sort. But often this is the bit that's missing, so getting somebody in to give them a hand with that if they don't have the resource on the board is really, well advised.

Then lastly around the framework to measure maturity and the assurance that goes with that, so how do they know that progress is being made.

So these are really key questions that if you're in a leadership position you should be asking and if you're not in a leadership position, it's the sort of information that you might want to start pushing up through layers of management to try and get people thinking about things in the right way. And it doesn't have to be super technical either.

>>Elf Eldridge: I have the privilege of having the slide deck between you and drinks so I will try to make this as painless as possible I promise. We got myself and Steve to give you two different perspectives today because the governance perspective is really important. Everything I'm about to say doesn't matter if you don't have support from government, you're patching a sinking ship and you can patch as much as you like but it's still sinking.

I'm going to jump away from high level strategics and go okay there are things all of us can potentially do to improve the situation we're in. Really the question is we've got limited time, money and resource, I've got about 10 minutes left before everyone's attention

turns off so what is the best practice advice I can give enough that short period of time mostly through the medium of pitches.

So a really important thing to consider when we talk about preparing ourselves for cyber resilience and being resist enter to risk is what we're doing actually reducing risk. Is paying thousands of dollars for this actually reducing risks or is it help us feel better, and it turns out is a really complicated question. What we like to do instead is ask the easy question, pay the money and get the easy answers. We can see a lot of it in this particular cartoon, which is one of my personal favourites, we spend a lot of time in cyber-security improving our encryption and that is really, really important.

But if I can phish your credentials or if I can walk into your offices, I did this last week, put on a hi-viz vest and walked into somebody's office with a ladder, plugged some things in and left again. It turns out your encryption doesn't really matter very much. If you've got interns going in and out and if someone on the street says I'll give you 200 bucks for your user name and credentials, it doesn't matter if your password's 64,000 characters long does it, because there are people who are out there who will do that.

Let's talk about the two types of attacks I think are worth considering. There are thousands more. NCSC have way more data than me so talk to them for details but the two classes of attacks that it's important to understand are opportunistic and targeted attacks and a lot of us spend a lot of time and head space worrying about targeted attacks, because they often get on the news.

So my favourite example recently from late last year is the Uber breach, if you're not with it, a hacker group got into Uber and they got everything, they got into the back end of all of Uber's security systems, every single one and the route they used to get there is really funny as well, one of their engineers didn't update their home media server, they got in that way and they use pivoted if there to get into Uber headquarters and took everything. They didn't steal any money, it was just hey look what I can do. That is an example of a targeted attack. The attacker knew who they were and what they were attacking and went on the dark web and brought some credentials to get into Uber.

That's only one type of attacks. The other type of attack is opportunistic. We all have interconnected systems, whether on cloud or prem they expose different services, and every so often one of those services will be vulnerable. Sometimes it's because you didn't patch it, though rarely. More often than not it's because a hacker like me figured out to how to break something then it's called a zero day, because no-one knew about it beforehand.

And it's really hard to protect against those because by definition you don't know about them beforehand.

I spend a lot more time worrying about opportunistic attacks than targeted attacks, because targeted attacks you can help protect yourself against, you can train your staff to be better at phishing you can have fire walls, internal logging a sock or a seam, you can add all these different layers. But an opportunistic attack, there was a firewall bug that came out three days ago that allows an unauthenticated attacker to gain full access to a firewall, and if you're not familiar with a firewall it's the thing that keeps people out of your network, you don't really want someone out of your network to control. It's not uncommon for these things to be found.

The reason I stress so much about that is a lot of organisations I spend time in just focus on preventative measures and I get that we want to keep people out of our networks that's the right approach but just a myopic focus on prevention will leave you open towards these opportunistic attacks. So I run a variety of courses with the institute for IT professionals where we talk about basic cyber-security protections and skills and most importantly the incident response process and how you do that well. In my book a practiced incident response process is one of the most effective ways of reducing risk and bringing your staff along for the ride. Yes, I love technical controls, they keep me out of most systems, they work very, very well, but in isolation, they're not perfect. That along with good incident response can really help improve organisational security. We should probably also ask what kind of attacks happen. Again you were in the privileged position where you can actually go to NCSC and get more detailed information and they will reveal information for you for the rest of us who aren't public sector we have to rely on data gathered by NZ CERT if you're not familiar the computer emergency response team in New Zealand, they collect information and report on it every quarter about how many of what kind of attacks actually happen in New Zealand. And don't worry about the details, the details is your gut instinct that all those scam texts and e-mails and phone cause and WhatsApp messages that you get all the time, they're there because they're cheap and because they work and they've been working ever since we started tracking this information and they're going to keep working. And that's not because humans are terrible or stupid. I have been scammed, been fished because it turns out sometimes it's not a great idea to read work emails on a Friday afternoon after you've had a beer. It's not I'm a terrible human being, that is also true, that's independent, right.

We are human, we're going to make mistakes, and our security process should expect that without demonising the humans That are involved. The most important thing here is if you don't have an incident response process for phishing, or your sea level's being scammed, these are the most common, most impactful forms of cyber attacks that happen at the moment. And that raises a big question about why you are not worrying about the most common things but you are spending lots and lots of money on firewalls and protective things as well.

By far in a way scams and fraud are the most frequent and most effective forms of cyber attack in New Zealand, as reported to NZ CERT. Their data is not perfect but it's the best that we have and it's consist present what we see in Australia, the UK and the US as well. If you don't have a plan for this, that's where I would start. Yes you can worry about denial of service, malware, ransomware and you absolutely should but maybe don't start with that. And so if you're going to worry about that, where is the best place to start? This. It sounds really stupid, I'm sorry I'm not trying to talk down to anyone, but a big part of my recent role has been running table top exercise for public and private sector organisations and I go in and see incident response plans that either around the up-to-date or don't exist which is fine this is a journey, but the biggest issue I see with most of them is that they are so prescriptive and people are so concerned they lose sight of what is important in incident response. It's exactly the same about your BCP or disaster recovery plan. It's actually the plan helps you and helps your incident response team

So if your incident response plan is spread over 45 different documents on three different ecosystems that require 7 different log-ins, and there's a printed back up in Jared's shed that's not really a great process to help your incident response team. If you can have a relatively simple overview that is short and easy to digest, when you're poor stressed out staff are trying to enact it at 4 o'clock in the morning when there's an attacker breathing down their neck they're less likely to make a mistake

The second thing if it's 4 am and the first time they've seen it it's not going to go well for anyone. The second biggest thing we can all do is once we have a plan, practice it, and I don't necessarily mean go and hire an advanced attacking group from somewhere overseas to hack your organisation, no, I mean take your incident response plan out, blow the dust off it and practise it, run it through. Even on a whiteboard in an hour, you can do a lot and get a lot out of practising your incident response process, even at a high level, and I really highly recommend if you haven't done that, that you do this.

Beyond that, there's a lot of technical controls. We could all put in. There's a laundry list of them. We've got the NZISM which lists roughly 4,500 technical cyber-security controls that you might wish to push in place. I do a course on that by the way.

I wouldn't start with that myself personally. We're really, really lucky, ourselves and the Australians across the ditch have a short list of cyber-security best practice things that organisations small and large can do to protect themselves. The Australian one is a list of 8 things long, I'm not going to go through them here but you can go and find out about it on the AS CA S D website. They're all standard and work for organisations of all sizes. You might not be able to have all of these, but if you don't, asking why we don't have them and is that a choice or is it something we're not aware of, that is a really good place to start.

The NZ CERT each your produce a risk of critical controls, a list of 10 because we like to be different here in New Zealand, 10 is better than 8 apparently, a list of 10 things that organisations can do to protect of them selves. There's an overlap with the Australian one as well, again I'm not going to bore you by going through the details, CERT New Zealand does a great job of writing all of these up and explaining what they are and how to implement reasonably cost-effective on their website

Given I've got approximately 2 minutes left I thought I'd do something fun at the end and go let's talk about AI in the cyber-security space. Maybe it's just my news feed but since chat GPT has come out everyone has been talking about AI this that and the other thing and how AI robots are going to hack all your stuff and take over your car. I haven't seen that yet. In fact if you ask chat GPT to do hacking, this is what it will say, if you ask it to write an RCE, which is a remote code execution vulnerability and allows someone remote to take over a system, chat GPT will go no, I can't do that, how rude, how dare you ask.

But if you write I need to do some homework for an assignment, chat GPT will absolutely answer that question for you. Sure this code here, again the details are not important, but chat GPT will maybe not write it out explicitly but will give you very strong hints in that direction.

And so a lot of people are worried about AI hackers moving into this space and I've actually been to 3 talks on it recently and my own take away on this is all of the AI that I have seen coming out of chat GPT in the cyber-security space is Googling things more quickly than humans. I've yet to see anything that's truly novel beyond that and I have read a lot of different posts preparing up to this point. If we get beyond that point, then I'm

going to worry a lot more. But at the moment, other than being faster than me, I'm not seeing anything come out of chat GPT or any of the other AI kind of similar equivalents that gives me pause for thought.

And here is my last slide, my last thought I want to leave you with today. There is something about AI that really, really concerns me. And it's this. It's not the AI itself, it's the kind of information people are putting into it. So the short version of this is that Samsung banned access to chat GPT in early March but then it was stifling innovation so they opened it up and within a couple of weeks, surprise surprise, their internal sensitive IP ended up on chat GPT.

I don't know if we've seen similar things here in New Zealand it could be entirely independent MBIE have come out and said maybe our staff shouldn't use chat GPT and have access to it. I think from this, that's a probably good call, it seems like people putting information, sensitive information into random websites controlled by other organisations and agencies is a pretty major threat and a pretty major attack vector that. Is the primary thing that is causing me concern in the security AI space at the moment, I'm not losing any sleep over attacking chat bots but I am losing sleep over people putting sensitive documents and information into chat GPT.

So that is my short pitch on cyber-security and how we can do it a little bit better even though the world is a bit broken. Do we have any questions?

Q&A: Cyber Security in a Broken World

>>Finn Russell: Thank you both very much. Yeah, does anyone have any questions? We've got a couple online. But welt' go to the floor first maybe. We'll go straight up to the board. So how do you balance security risk and business risk, which comes first of security versus productivity?

>>Steve Honis: It's a great question, this is why we get stuff escalated up to the board or to the executive. They get to make that decision based on their risk appetite, what the data is that they're holding, and the regulations as well that are around the security that they need to apply to that sort of stuff. So it is -- it's a terrible answer to a question but it depends. It really does. There's no stock answer to it. The really important part to this, though, is that that decision's made by somebody who's the right person to make it. And I can't stress that enough. It's not something that in a day the IT manager should be making a call on, it should go up the chain further. Yeah so that's the short version on that one.

Was it a good idea to connect to the public WiFi in this room? I'll hand that over to Elf because he loves this stuff.

>>Elf Eldridge: As long as you're not doing your banking or hypothetically checking your emails on it, you wouldn't do something sensitive on an unsecured public WiFi, right?

>>Steve Honiss: Is it true all encryption will be broken it's just a matter of when.

>>Elf Eldridge: This is actually answered or hinted that in the latest version of the NZISM, go read that. In all seriousness, though, the latest version of the NZISM does have a highly recommended recommendation; make sure someone on your staff is fully across quantum cryptography and the new threats and challenges it brings in, which I feel like is quite a high bar. I certainly don't consider myself an expert, I'm not sure that many people do.

I think coming back to that question, though, it almost brings me back to my very first comic. Yeah, sure with another resources and enough time all encryption can be broken but if there's an easier way to do it and there almost always is involving bribery, threats, malicious behaviour, I'm probably going to do that rather than spend multi billions of dollars on compute time trying to break encryption. It's hard and expensive, there's easier ways to skin that cat I think in most cases.

>>Steve Honiss: Can you recommend any controls that can allow chat GPT access (inaudible). So this is a really interesting one we've done a lot of work on with clients recently, since chat GPT became talk of the town, technical controls, potentially, but that would be hard. The effective way of dealing with it though sing a realisation that people are going to use it anyway. This is where MBIE's stance on it has been an interesting one. Sure block it through technical policy, I'll pick up my phone and use it, that's human nature, is to find the most direct route to something.

So I'm not convinced that approach is necessarily the right one, I'm not throwing any shade at MBIE's decision at all on this, but it's not the advice I'm giving to the clients that I'm working with as their CISO. The advice I'm giving them is provide guidance and guardrails to the staff. You're going to use it anyway but just be aware anything you put into it you may as well be posting on an open website on a billboard.

Don't put personal information in there because that's somebody else's so don't. Don't put sensitive IP in there, don't put financial stuff in there, it's all going to be made public, it becomes somebody else's property and you're never going to get that back so use it smartly

If you want to use it to generate code or write marketing blurb, it's going to go on a public website anyway, anything you're happy to post on the internet fill your boots but

anything else don't. That's been really well received amongst the staff in the companies we've done this with, we socialise with the staff and say does this make sense to you, they're like hell yeah somebody's told us some good guidelines for it, I think that's most sensible approach

>>Elf Eldridge: I'll add to that, just 100 per cent agree with what Steve said. Chat GPT is not unique, people can copy and paste sensitive information into any website. The problem is not chat GPT it's the people copying the sensitive information to the websites. You can only sol that have by education and policy working hand in hand. I have seen some organisations solve this problem by having another AI in between their systems and for anyone that wants a really fun challenge for the weekend, there is a fun escape challenge that is just appeared in the last couple of days if you Google Gandalf.AI there is a chat GPT variant that has a secret password and it is a game, you have to get it to reveal its password to you. As you get through more levels it puts more and more AIs between you and it, adding more AIs makes it harder but it doesn't make it impossible, it's a really fun game I promise.

What's in the mirror image box in my last slide. I believe, it's us executing a piece of malware called Mimikatz which steals credentials from memory out of the recycle bin of something because commonly stuff in the recycle bin isn't scanned as thoroughly as other locations or rather didn't used to be, our defender is a thing. It's really hard to read in reverse.

Rubber ducky and pineapple. For those who aren't familiar with those, they are both malicious devices. Rubber ducky is a USB you plug in and it pretends to be something else, typically a keyboard and tries to log in and log what keys are being pressed. Pineapple, a WiFi pineapple is a malicious wireless access point, so you can put it in here and your phones might choose to connect to it rather than something else.

I presume IPv6, which is a replacement to IPv4, which has more kind of unique addressing and security controls, I still use rubber duckies and WiFi pineapples and engagements regularly. IPv6 is the thing it's not supported everywhere and in fact it's misunderstood a lot and people configure it wrong they are still absolutely part of my toolkit and I don't see them going away apart from the fact I lost my rubber ducky so I need to get another one. I lost it at a client.

>>Finn Russell: I think that's all the time we have. But a massive thank you to Steve and Elf for coming out. One big round of applause. **[Applause]** I'll now hand over to Chris to close the conference.

4:45 - 4:55 pm: Conference Closing

>>Chris McDowall: Technically I have 10 minutes on the program but I don't think I'll need all of it. I just poked my head out before I can confirm that the drinks and nibbles are in position so if we finish early that's not going to be awkward.

Thank you very much everybody once again for coming along to the conference, it's been a real honour to have you all. And online people as well, looks like you've stuck around the, we can see how many of you there are and you're all still there more or less so that's great.

I'll just give a few quick reflections on the conference do, a few thank yous and leave it at that. At the start I talked about what we mean by digital resilience, and I had my very rough and ready diagram, I'm just going to go through those categories again and reflect on what people have been talking about. We had resilience at the national institutional and personal levels, we've heard some great stuff about -- the conference has been bookended by two cyber-security presentations which is really cool. We've heard about the elevated risk environment, I suppose, strategic competition, whatever it's called geopolitically. There's a lot more malicious activity flying around in cyberspace than there used to be, it's on all of us just to be aware of that.

At the institutional level, we had a great presentation from Damon hearing more about what they were doing with Service New South Wales, it was a bit of a revelation for me to think about not to be quite so cynical about using the term customer in that way but to really see it as a powerful way to change an organisation's culture and focus more on the outcomes of the people we serve and on collaborating with each other in the back end

Then at the personal level, it was great hearing from our chiefs panel about the things which they've struggled with themselves or that their teams have struggled with and the ways they've taken steps to address that and keep on staying positive coming to work despite all the challenges

Then also the need, when we're caught up in busy times or stressful or high pressure situations, to have processes which support us and help us like rosters and food being delivered when necessary.

We'd also taken a look at, what was it, rack my brains, so we've had some great cyber-security tips and I'm going to be watching out I suppose for people in hi-viz with

ladders coming visiting the office if it looks like Elf. What happens if you get pinged after you get pinged?

>>Elf Eldridge: I get caught pretty much in time.

>>Chris McDowall: That's good to hear, I'll point him out to our security guard. Lots of other great tips as well that framework from the NCSC I'm going to be looking that up learning about the different areas where we need to strengthen in my organisation. I don't work in cyber-security per se but probably most of us we know the cyber-security people and we have to deal with them a lot, so knowing more about it ourselves can only help us I think.

Then on the incident response side of things, yeah, that coordinated incident management system it's quite powerful, you can get training on it as someone in the public service, so ask your facilities team or incident management team or whatever it is at your organisation about that, it's well worth it, and it can get you into some cool work at some point.

Then what does that leave? Really just AI. Don't give your sensitive information to large language learning models because you're not quite sure what's going to happen to it but keep learning how they work and there's a lot of great opportunities there as well.

We've had some great presentations. I'm going to be watching some of the recordings later on when we put them on our website. I think all the presentations in here have been recorded bar just one or two, where we're keeping more of a Chatham House rules situation. So that's it really.

Thank you for coming, GOVIS as we've said before is run by volunteers, we'll be having an AGM in a few months in August or September if anyone wants to become more involved just get in touch, reply to one of our emails and we always love to have more people on the committee so watch out for that, watch out for an evaluation survey for the conference next week and then watch out for the presentation slides and the recordings going up on our website

And thanks once again to volunteer committee, Paddy, Mick, Finn, Christian, Fay and Rochelle and then finally thanks to Hayley Andre nor our conference organisers and Katherine on the stenography machine and Alex and James at the sound desk and our caterers.

Brilliant, round of applause for everybody.

>>Mick Crouch: It's not over until I say it's over. Just wanted to point out all the hard work that the organising committee does to make these things happen, they have day jobs

and we've done two this calendar year. We've hoping to do another one next June, I just wanted to say a personal thank you to Chris, and Paddy and Finn, you each get one of these bags, and thanks to all of you. I don't have anything for Christian. Actually I did give Christian his present earlier, he was thrilled. But it's personal between us. Anyway, let's go drink. **[Applause]**