This document is a report by the Cyber Security Advisory Committee (CSAC). The CSAC was an independent industry advisory committee, appointed by Ministers.

This document does not represent government advice or government policy.

New Zealand Cabinet Cyber Security Advisory Committee Report back on Workstreams 1/2/3

24 March 2022

Introduction

The Cyber Security Advisory Committee (CSAC) was convened by Ministers to provide independent advice to Cabinet on options to improve cyber security in Aotearoa. CSAC was tasked with providing ideas, advice and options to Cabinet on:

1. *Lifting the cyber security capability of the private sector and its resilience when under threat;*
2. *Providing recommendations around a scalable cyber security framework for New Zealand companies and organisations;*
3. *Providing insight and recommendations around the customer orientation of government agencies working on cyber security matters; and*
4. *The design and establishment of a permanent public-private collaboration forum on cyber security with the aim of better connecting and harnessing the New Zealand cyber security ecosystem.*

This paper provides recommendations for workstreams 1, 2 and 3.

Guiding Principles

CSAC adopted six principles in tackling the workstreams in its Terms of Reference (ToR):

- Frankness of advice.
- Tikanga is central. We recognise the principles of Te Tiriti o Waitangi and the relationship between iwi/Māori as tangata whenua and with the Crown and its agents as tangata Tiriti.
- No panacea. The diversity of companies and threats means no 'one-size fits all'.
- Investment ready. A significant lift in capacity will require significant investment.
- No blueprint. The ToR did not ask for an organisational blueprint.
- Global connectedness. We believe New Zealand should maintain cyber resilience at the level of Five Eyes partners.

Core recommendations

While our full set of recommendations are outlined in the following sections. CSAC has six core recommendations:

1. **We recommend the creation of a 'single front door' providing companies and organisations a single agency for reporting attacks, obtaining meaningful advice around response, and accessing practical help in recovery.** Whether an umbrella service, the reworking of an existing agency or a standalone agency, a 'single front door' would avoid the confusion, crossover and gaps experienced by many

victim companies, significantly improve user experience and work with outreach partners to help lift resilience. This was a unanimous recommendation across the three workstreams. A key resource for the new entity will be up-to-date playbooks on common attack vectors including DDoS/malware/ransomware with real-world advice on mitigation and response.

2. **We recommend specific recognition of impact and loss across all 'capitals', including cultural capital.** Data and privacy are major issues; effective cohesion between cyber, privacy and data protection guidelines and regulations is vital. Māori data governance and data sovereignty is also an overlooked and significant issue. Several work programmes within DIA and Stats NZ are currently considering the Data Strategy and Roadmap for Aotearoa New Zealand. Indigenous approaches to transforming the data ecosystem are being researched as part of the Endeavour-funded Tikanga in Technology project. Any cyber frameworks should be co-designed with iwi and Māori while contemplating New Zealand's obligations under the UN Declaration on the Rights of Indigenous Peoples. CSAC strongly recommends a separate, suitably-resourced workstream be established by DPMC to oversee this.

3. **We recommend the implementation of minimum cyber risk management guidelines for companies, expressed as a simplified form of the widely-understood NIST Cybersecurity Framework.** This 'NIST Lite' framework would use the top line typology of Identify/Protect/Detect/Respond/Recover. These guidelines would create a common language of risk control, while providing a structure for advice, capability development and support.

4. **We recommend the introduction of mandatory reporting of cyber incidents and ransom payments for those organisations and sectors upon which society relies.** In addition to the existing organisations of national significance this should be expanded to include Internet service providers (ISPs) and relevant managed ICT service providers (MSPs) along with key sectors such as food, transport, health, education and financial services. Enabling tools such as NCSC's Malware Free Networks (MFN) and CERT NZ's Phishing Disruption Service should be expanded to accommodate all of those qualifying businesses.

5. **We recommend sustained investment into building cyber capability and capacity in the labour market**, through a programme of work visa changes and funding of public and private sector cyber education at academic and trade level.

6. **We recommend a strengthened oversight regime for ISPs and MSPs** with regard to their capability and their controls of cyber security risk. ISPs and MSPs should also be subject to mandatory cyber incident reporting requirements. Given these companies control many of the 'roads and pipes' that bad actors must pass through to commit cyber-attacks, they have a great opportunity to contribute to better outcomes for business and consumers.

Detailed findings of all three workstreams and their full recommendations are outlined in the sections below.

Workstream 1 Findings – Lifting Private Sector Capability

Overview

Outside the cyber security sector, little is known about the extent and make-up of threats facing New Zealand businesses and consumers. DDoS and ransomware attacks dominate media attention, particularly when it affects everyday lives, as in the case of the Waikato DHB or bank attacks. However, this fails to capture the size, complexity and level of organisation that sits behind the cyber security threats. In particular it misses the role of state-sponsored attackers, professional cybercriminals or the world of malware-as-a-service. This disconnect may be leading to the public downplaying the risk or assuming government and the private sector have it covered. The reality is that no-one has it covered, and thousands of attacks are being inflicted on New Zealand businesses every day. Meanwhile, for a small business operator in a time of pandemic it is challenging enough to get through each day of trading without having time to worry about what might happen on the internet.

In a world where everything from beer fridges to burglar alarm systems are connected online and can be controlled from a mobile phone, network attack surfaces are expanding. These are likely to expand further with the growth of cyber-physical systems, open-source code, cloud applications and social logins. As Gartner recently noted, businesses need to look beyond traditional cyber security approaches to manage a much broader range of security exposures.

We understand government is already looking at a centralised response to Internet of things (IoT)-related threats and 'soft underbelly' attack vectors, so have not formed a specific recommendation in this area. However, we note the urgency for developing a scalable approach, which may include establishing standards at a national level for web-enabled hardware sold in Aotearoa. For consumer devices (such as routers or IoT) this could be similar to the consumer tick model where hardware is rated for its cyber protection – for the benefit of both the individual's protection, but also to reduce the likelihood of these devices being infected and leveraged by bots to expand a bad actors computer power and widen the distribution of attacks closer to home. Additionally, CSAC encourages government to provide recommended approaches for companies in terms of cyber asset attack surface management as part of any future cyber security framework.

More broadly growing New Zealand's cyber security maturity is critical to the success of our economy. This is challenging when risk awareness is low, and negative consequences are dismissed as being unlikely or covered by a third party such as a telecommunications provider or insurer. Brand reputation is considered the greatest asset to protect in most of the larger cyber-attacks; and for some victims may invoke whakamā, with its associated feelings of shame or embarrassment. These factors may limit what data is shared and/or reported.

Shared knowledge is limited to those parties bold enough to speak publicly, further reinforcing the general perception that cyber risk is tolerable at present levels. Board and senior executive oversight is variable and the treatment of cyber risk as core business risk is generally limited to larger organisations. Lack of cyber oversight as a cause for claims of director and officer negligence has not yet been tested by prosecutions in Australasia. Looking at parallels from Health and Safety may be instructive here, in that these considerations were not a priority until regulatory controls were put in place requiring minimum standards and clearly defined governance liability for negligence.

To date, agencies have largely focused on awareness-raising programmes to improve to improve resilience. These have had little urgency, impact and failed to reflect a Te Tiriti view. As a result, we do not believe these awareness campaigns have driven discernible change in New Zealand's cyber resilience. A recent report from Gartner suggests that the ineffectiveness of cyber security awareness programmes is not just restricted to New Zealand. Meanwhile where businesses do engage with government agencies, our research shows their experience is generally unsatisfactory.

All of this contributes to our belief that awareness raising and educational programmes are of little use, so systemic change is needed. Capacity and capability to manage and respond to cyber risk must be part of any worthwhile plan for improved resilience. This is a pertinent issue as both the private sector and public sector cyber agencies continue to grow their talent base, creating a highly competitive market for appropriately skilled staff in a finite and overcooked labour market.

It is prudent to consider the broad pool of talent New Zealand will require if it is to sustainably maintain adequate defences, along with any additional objectives for economic and wellbeing growth through digital excellence. An appropriate balance between tertiary, trade and specialist education will need to be made, informed by the different needs of the private sector and of government. Identifying and promoting transferable skills and opportunities for cross-training would also provide significant benefit. Importing talent from offshore via more flexible work visa structures will be an important aspect to this, and is critical in the short term.

CSAC believes that the private sector is able to significantly increase cyber capacity (as it has already done) through on-the-job training, recruitment of offshore talent, coaching and delivery of focused training courses for specific skills as in the case of the Kordia Cyber Academy. Incentives should be balanced to support the private sector to innovate and invest in this area, while maintaining a robust pipeline of support for public funding of cyber qualifications. An effective programme for capacity development should be developed through comprehensive private sector engagement.

While the current system has agencies that could help consumers and small business lift capability these are not performing at the scale required. Nor are these agencies operating in a manner where their purpose, public facing 'story' and scope is obvious. For this reason, our recommendations for workstream 1 revolve around a single front door along with a Te Tiriti informed approach.

Workstream 1 Recommendations

CSAC makes five recommendations in support of workstream 1:

1. **We propose reorienting the public facing elements of government by constructing a 'single front door' for cyber security.** Whether as an umbrella portal, a standalone agency or embedded in an existing agency; this would need to be well defined, resourced and hold the budget required to achieve a comprehensive support infrastructure. Importantly it must be victim-centric to give meaningful support. Investment should be commensurate with other Five Eyes countries. Based on the investment quantum in Australia and the United Kingdom and adjusted down for local scale, this suggests an additional annual spend of between $200 million and $300 million.
2. **We recommend building an outreach arm** into the single front door. This single front door should be empowered with funding and a clear mandate (which could be a statutory requirement through empowering legislation) to partner with the community organisations currently providing cyber security support at the coalface for SMEs. This includes accountants, lawyers, Citizens Advice Bureaux, technology retailers/vendors (including mass market retailers such as Noel Leeming and PB Tech) and Software-as-a-Service (SaaS) providers like Xero. These partnerships could also include Iwi/Māori organisations, chambers of commerce, regional business networks and the EMA, along with trusted advisors such as ICT security consultants.
3. **We propose the single front door gives effect to Te Tiriti o Waitangi.** This includes co-design of a reimagined approach with Māori to ensure that the single front door provides services to iwi, Māori and Māori organisations that are culturally competent and responsive. It also must recognise the loss of cultural capital as well as financial capital.
4. **We recommend direct intervention to strengthen capacity and capability within the cyber security labour market** through migration, training and working with education providers. This would include

informed changes to work visas for cyber professionals and expanded funding of private and public sector cyber education (particularly at the operative/trades level).

5. **We recommend a review of the operation of cyber insurance in New Zealand be conducted by RBNZ as the insurance oversight agency.** Currently cyber insurance is poorly understood and poorly utilised (see Appendix 8). Meanwhile premiums are increasing while coverage is decreasing, and we have heard some concerns about brokers' selling techniques. All this comes at a time when global players are reducing their exposure to the market. This is also potentially a missed opportunity to raise capability. This could see businesses applying for cyber cover being required to undertake a risk assessment. In order to get cover, or reduce premiums, shortcomings will need to be rectified, lifting capability as a result. The RBNZ review could usefully snapshot the current state of the market when it comes to cyber insurance in terms of product, pricing, coverage and distribution (including the role of brokers); as well as evaluating the potential to raise resilience through required risk assessments.

Workstream 2 Findings – Cyber Security Frameworks

Overview

The New Zealand Government has invested significantly in the provision of useful and relevant cyber security advice, guidelines and suggestions through its various agencies. In general, the content is of good quality and if applied is likely to offer useful strengthening. However, access to the content appears to rely on the user knowing where (and why) to find it. It also assumes a level of sophistication in terms of interpreting what might apply for a given company. The portals for accessing this information require a degree of navigation and old-fashioned modes of interaction. In some cases, this extends to the completion and despatch of Word documents, which feels clunky for cyber agencies.

The content appears to be structured in a government or Ministry-centric way, rather than reflecting the user-case of the site visitor. Guidelines provided between CERT and NCSC, while robust on their own, are divergent and there appears to be little directive guidance for those simply wanting to know where to start. There is also a lack of practical advice on the most common attack vectors and effective ways to respond, recover and future-proof.

Locating information on what to do in the event of a cyber-attack appears even more opaque. Successful mitigation of active attacks appears to rely on professional advisors (like ISPs, insurers or specialist providers) navigating the support pathway for an affected company (including the path through government). Without 'friends on the inside' it can be tough to enter the government support system when attacked, unless the attack is one that meets the NCSC's test for being 'nationally significant'. While the organisations that make up the control ecosystem are sympathetic to companies who have been attacked, there is no clear pathway of approach and response. Indeed, some officials we spoke to were themselves unclear on what they could or couldn't do to help victims. A lack of 'playbooks' for common attacks (such as DDoS attacks) is often cited as a gap, as is the ability to discuss management options for common attack vectors or get meaningful advice on communications (see also workstream 3 results).

In addition, ISPs and service providers have no mandatory reporting requirements, so only limited information and learning from attacks is shared. Decisions regarding whether to pay ransoms, how to respond to cyber-attacks, the effect of attacks upon some companies' continuous disclosure obligations and the impact of any publicity appear to be made on the fly. Although CSAC understands that every cybercrime is an offence against the Crimes Act 1961, NZ Police themselves note that "no agency has the function of collating national incidents or statistics". The lack of data is a serious gap.

Immediately prior to the delivery of this report the SEC in the United States announced a proposal for mandatory material cyber security incident reporting. The proposal contains a requirement for listed companies to immediately disclose material incidents and to deliver periodic reports to the market on previous cyber security incidents.

Here in Aotearoa the NZX listing rules are based on the principle that any event that could be reasonably be considered to have an impact on share price must be disclosed immediately. The listing rules don't draw out or highlight any particular type of event. This means those cyber-attacks which are successful and have a material effect on business operations are implicitly covered. We understand two successful attacks have been disclosed in the last year.

We are not in favour of making it an explicit requirement in the listing rules or any other mandatory reporting framework to publicly disclose material attacks and incidents. This is because it could have the effect of encouraging companies to opaque reporting of incidents, could unfairly affect investor sentiment and is very likely to aid the hackers. CSAC favours a requirement to privately disclose material incidents to the new single front door. We note such a provision for private disclosing of incidents already exists in the Privacy Act in respect of reporting certain events only to OPC.

Looking more globally, we note that New Zealand appears to have fallen behind its Five Eyes partners with respect to introducing stronger oversight and risk controls in the cyber risk landscape. Those who provide internet services and internet access are key control points for effective cyber defences and there is little or no oversight of the performance and competence of these providers. New Zealand presently lacks any mandatory requirements for reporting of cyber incidents (other than those agencies that are mandated to by the NZISM), whereas in the UK, Australia and the US such standards are being introduced for critical sectors. ISPs and MSPs should be included in any new mandated approach.

CSAC does not consider it is the right advisory body to be mandating specific standards to which companies and organisations should adhere. Indeed, CSAC does not consider imposing mandatory risk management standards would be useful, nor do we think one framework is likely to meet the requirements for all organisations. Instead, we believe incentivising adoption of a guideline for minimum expectations for businesses, supported by providing best practice framework recommendations and mandatory reporting of critical data under certain circumstances will drive positive change. The Health and Safety at Work Act 2015 (HSWA) changes provide an example of how this can be done without the burden of oversight, cost or bureaucratic inertia. Incentives to do the right thing are likely to work better than being punished for doing the wrong thing.

Lack of strong data governance and data oversight rules, particularly in association with Iwi and Māori data, is a useful opportunity for improvement. While beyond the remit of CSAC, the lack of a strong data governance framework that represents a Pākehā and Te Ao Māori view is a weakness. CSAC recommends a separate initiative be taken to develop this.

New Zealand has unrivalled foundations to create best practice cyber resilience for itself and its partners. We have a reputation as a high trust nation, are a member of the Five Eyes partnership, and through iwi and Māori partners can affect a world-leading Te Ao Māori-informed data governance lens. We also have just four pipes joining us to the terrestrial internet.

The good news here is that Aotearoa has a strong economic opportunity to be a leading digital marketplace. This is by virtue of strong cable connections to world, large investments in data centres being made by AWS, Microsoft and others, clean energy sources, strong trusted partners on global stage, high levels of education, and being considered a safe place to host data. It's time to capitalise on these competitive advantages.

Workstream 2 Recommendations

CSAC makes six recommendations in support of workstream 2. The recommendations consider both systemic frameworks (i.e.: the organisational system) and control frameworks (i.e.: control methodologies).

1. **We propose the creation of a single government front door for cyber security for all organisations, agencies and individuals**. Establishing a well-funded, independent Crown entity accountable for cyber security oversight should be considered to sustain change. This could take the form of a well-resourced portal stretching across the key players in the system (NCSC, CERT, NZ Police), a new standalone agency or it could see one of those players having their mandate changed to provide a victim-centric response. Good resourcing here is key. As an example of current resourcing, we understand that NCSC has limited ability to provide incident response services to more than two C2 level attacks at once. This is below the level needed now and in the future.
2. Develop minimum cyber risk management expectations for companies and organisations, expressed through guidelines that use a common language. **We recommend a simplified NIST Cybersecurity Framework (CSF) outline as the overarching framework**, used to create a common language of cyber risk management across large and small organisations and companies. This will necessitate some realignment of the language and content - though not necessarily the underlying methodologies - employed by agencies such as NCSC and CERT. For smaller organisations, adoption of the CERT Critical Controls provides a useful level of cyber protection without a large administrative impost. Adopting a simplified NIST CSF would also allow a single and common risk assessment framework for NSOs,

something that is currently missing. It would also provide a framework for measuring resilience across smaller businesses. To be clear, 'NIST CSF lite' would be recommended not required.

3. **We recommend that mandatory reporting of cyber incidents and ransom payments are implemented for those critical organisations and sectors upon which society relies**. This would see the creation of a broader group than just the NSOs. It would be expanded to include such sectors as transport, finance, energy and grocery. From what we understand, this would be effectively a fivefold increase in companies required to report. In implementing this, the risk of censure as a result of self-reporting must be understood and balanced with the need for more reporting. It could also see the expansion of the application of NCSC's Malware Free Networks system and CERT's Phishing Disruption Service.
4. **We recommend a strengthened oversight regime for ISPs and MSPs** with regard to their capability and their controls of cyber security risk. ISPs and MSPs should also be subject to mandatory cyber incident reporting requirements outlined above in recommendation 3.
5. **We recommend the New Zealand Government as a minimum maintains cyber risk management and regulatory parity with its Five Eyes partners**, but ideally looks to innovate in this area as some of our partners have done. An example of UK innovation is the significant investment by UK NCSC into incentives to increase cyber capability in the private and public sector, along with targeted and proactive information for different sized companies. They also operate online communities for private sector professionals. Our understanding is that on a pro rata basis, New Zealand cyber security agencies are significantly underfunded compared to their Five Eyes counterparts. CSAC recommends that the budget and number of staff allocated to national cyber security defensive and advisory roles in our Five Eyes partner agencies (scaled for size) be reviewed against current budget and staffing levels in comparable New Zealand agencies.
6. **We recommend specific inclusion of a Te Ao Māori-led perspective** into national standards for cyber protection and iwi and Māori data governance. This could be an adaptation of existing global best practice guidelines (such as NIST CSF). CSAC recommends a separate workstream be created to review this, possibly coordinated in line with the current Tikanga in Technology research underway.

Workstream 3 Findings – Customer Orientation

Overview

CSAC developed a survey combining quantitative and qualitative components which was used to carry out telephone/video interviews with 20 companies who had experienced cyber attacks in the preceding 14 months. The participants include small, medium and large companies as well as security specialist firms and Māori enterprises. We note that it proved difficult to get Māori enterprises to participate, so these perspectives are not as well-represented as we had hoped. The one survey we did do in this area suggested there are challenges unique to Māori enterprises and this is one of the reasons we have recommended further investigation in this area.

Sizing up the attacks

- The most common types were ransomware (25%), DDoS (22%) and phishing/social engineering (16%).
- Ransoms were involved in 61% of attacks. Size varied hugely - from $47,000 to $60 million. We also had unverified reports of higher figures. 56% of reported ransom demands were made in Bitcoin.
- Attack duration averaged 73 days with recovery time a further 40 days, but both varied from one day to one year.
- The cost of defending the attack ranged from $5,000 to $20 million, while the new ongoing yearly costs averaging two thirds of initial response cost – i.e. an attack that cost $1 million to repulse typically results in new ongoing costs of approximately $670,000 per annum.
- While attack victims dealt with up to nine government agencies, the main four were CERT, Police, NCSC and Office of the Privacy Commissioner (OPC). 'Merry-go-round' experiences were common between these four.

Customer Orientation

- Of the main four agencies, OPC had the highest consistent ratings around service and customer orientation. They were seen as focused, professional and helpful, scoring 80% or more across most measures.
- NZ Police were seen as fairly clear on their mandate, but not that useful, proactive or interested. Of the four core agencies they rated lowest overall in terms of customer orientation. Victims' comments suggest case management and follow-up were not ideal.
- CERT was very responsive but not seen as that useful, practical or proactive. Feedback suggests a mismatch between the generic services offered and the more specific resources desired. It is also unclear if MBIE – which we understand was meant to be a temporary 'home' for CERT back in 2016 – is in fact the right home.
- NCSC was also fairly quick to respond but did not rate well in terms of usefulness, practicality or proactivity. NSO companies found it difficult sometimes to know if they were dealing with NCSC or GCSB and some found the "firehose" of communications overwhelming.
- Many companies felt agencies were keen for their information but less able to provide meaningful help in return, resulting in a sense that companies may be better off ignoring government.
- The most sought-after resources were playbooks for common attack vectors, case studies of similar attacks, introductions to other companies who had experienced comparable attacks and specific advice on how to configure applications (Microsoft, firewalls, cloud settings) to translate CERT/NCSC advice into actual useable configurations.
- There was common appetite for practical advice on handling communications around an event – particularly social media and news media. Victim companies received no advice on this from agencies and consequently experienced overwhelmed contact centres, and found themselves outmanoeuvred by journalists.

- There was also strong appetite for real world playbooks of common attack vectors including DDoS, malware, ransomware and phishing. These need to contain good granularity. For example, a DDoS playbook would outline the basic way DoS and DDoS work, the difference between a DDoS and brute-force attack, the points at which you can intercept, common mitigations around URLs/static pages/moving to cloud/sinkholing/CDN mitigation, creation of a war room, harnessing partners, constructing customer comms and post attack bolstering.

Result Heatmap – Customer Orientation (green is good)

Agency	Average of How quick is their response to your approaches and requests?	Average of How useful is their response during attacks.	Average of How clear do you think they are on their mandate and what they can do for you and your	Average of How proactive are they in helping you after you make contact?	Average of Do they provide any practical assistance during the attack or recovery?
CERT	4.00	2.71	3.06	2.61	1.94
NCSC	3.73	2.73	2.55	2.27	2.09
OPC	4.43	3.75	4.14	2.75	2.60
Police	2.64	1.90	3.18	1.70	1.70
DIA	2.50	1.50	3.00	1.50	2.00
MBIE	4.00	1.00	3.00	2.00	1.00
RBNZ/FMA	5.00	3.50	3.50	4.50	3.00
Other	4.33	3.67	4.33	3.83	3.00

Key:
1 is low – 3 is medium - 5 is high

Result Heatmap – Getting the balance right (green is good)

Agency	Average of How was the balance of information flow - what you provided them vs what they provided you? (1/2/3/NA)	Average of Keeping in touch during the attack.	Average of Customer service orientation	Average of Overlap between agencies
CERT	1.65	1.59	1.65	1.94
NCSC	1.20	1.25	1.20	2.00
OPC	2.00	1.83	1.83	1.33
Police	1.25	1.00	1.25	1.29
DIA	1.50	2.00	1.50	2.00
FMA	2.00	2.00	2.00	1.00
MBIE	1.00	2.00	2.00	1.00
RBNZ	1.67	2.00	2.00	1.00

Key:
How was the balance of information flow -? (1 - in their favour, 2 – about equal, 3 – in my favour)
Keeping in touch during the attack? (1 - not little, 2 – about right, 3 – too much contact)

Customer service orientation? (1 – little/none, 2 – good, 3 – excessive)
Overlap between agencies? (1 – no overlap, 2 – little, 3 – major)

Qualitative comments

The full list of qualitative comments made by victim companies are listed in Appendix 10 and provides insightful reading. Analysis by the research company who supported CSAC in this work grouped the comments into five buckets:

1. The current lack of clarity leads to a 'merry-go-round' experience for customers
2. There is a need for agencies to provide targeted, situation-specific and up-to-the minute advice, rather than generic advice
3. There is a need for victim-relevant resources
4. There is a need to move from reactive to proactive approach by core agencies
5. There is a need for quality control/client management tools to deliver better outcomes for victims.

Closing comments

The current organisational landscape around cyber security is the result of organic evolution and reaction to external events rather than design, so it should be no surprise that there is opportunity for improvement, informed by a Te Tiriti-led approach. We note New Zealand's Five Eyes partners have made considerable investment in cyber strengthening over the last 12 months and have made sweeping regulatory changes to support this. Global cyber risk is accelerating dramatically, with some close allies facing sustained attacks from state actors in other nations. So this investigation is timely.

New Zealand's comparative advantages in digital capacity and resilience are at risk of significant erosion. There is no policy-level view of the challenges and responses facing Aotearoa New Zealand in respect of cyber security. This absence is not trivial. Likewise, there appears to be a mismatch between agencies' own perceptions of their victim centricity and the realities of external experience when it comes to customer orientation. This may be due to resourcing and/or a limited number of agency staff having had previous customer-facing private sector experience. Whatever the reason, it is clear that things need to change if the government wishes to protect people, business and the economy from cybercriminals.

Ransom payments are a vexed issue, as is the disclosure of ransom payments itself, from both national security and private sector governance perspectives. The New Zealand Institute of Directors, among others, is seeking clarity from government regarding its stance on ransom payments. Similar discussions are occurring in Australia and should be considered before changes are made.

CSAC's recommendations are a starting point and represent just nine weeks of investigation. We note that government will need to engage in meaningful consultation with businesses and organisations if they wish to push forward with them. Our mandated terms of reference do not extend to delivering an organisational blueprint for government, nor to reviewing the forthcoming Cabinet paper on Cyber Security: Strengthening Resilience in the Wider Economy. However, you may choose to give us additional terms of reference along these lines or others.

We note the great response we have had from the core agencies we worked with to produce this report. We have found all agencies responsive to our inquiries and keen to lift their game. While we received assistance from many agencies, in particular we would like to note the help received from CERT, NCSC and DPMC – plus the practical help from our allocated MBIE minders.

Ministers and Cabinet, we thank you for the opportunity to carry out this work and hope you find it of value.

Signed:

Mike O'Donnell (Committee Chair)
Jon Duffy
Sheridan Broadbent
Steve Honiss
Mandy Simpson
Vanessa Clark
Victoria MacLennan
Hamish Rumbold

Appendix 1 : Broader Context

Government agencies' perspectives and priorities

In addition to the responsible Ministers, officials from GCSB (NCSC), NZ Police, MBIE, DPMC and DIA presented to CSAC members at the inaugural workshop on their roles, perspectives and priorities. Key insights from this workshop as they relate to security frameworks for companies and organisations are detailed below (in no particular order).

1. Increased attacks, increasing pressure on support resources

Cyber-attacks are accelerating significantly. The World Economic Forum Global Risk Report 2022 highlighted cyber security failure as the top technological threat facing organisations worldwide. The report also highlighted a 435% increase in malware and ransomware attacks in 2020 alone. New Zealand has also seen a significant growth in sophisticated, large-scale domestic cyber security incidents (Waikato DHB ransomware, RBNZ data breach, NZX DDoS, Fisher & Paykel ransomware) and a 65% increase in incidents reported to CERT NZ during 2019 and 2020.

The growth of connected devices is increasing the risk surface for cyber-attacks. The lines between individual, SME and major enterprise risk are blurred as more processing is undertaken at the edge of networks, often outside of corporate environments, such as in the home.

2. Confused support landscape

An issues paper prepared by DPMC noted that organisations and individuals affected by cyber-attacks often find it difficult to access the various forms of help available to them. This difficulty is in part as a result of there being multiple agencies responsible for uplifting New Zealand's cyber security, coupled with the volume of advice and information available (see Appendix 3 - New Zealand Cyber Security Landscape), as well as a tendency to ask the victims for information rather than proactively work with them to help them resolve the attack.

There does not appear to be the level of data sharing or even shared insight that should be possible – and expected – in an economy of our size. CSAC members believe it unlikely a sufficiently robust level of cyber defence would be able to be achieved without appropriate data sharing between agencies.

The determination of which organisations constitute a 'nationally significant organisation' that gains support through NCSC or a non-qualifying organisation that gains support through CERT is not clear, even to those within the agencies themselves. In addition, human factors – user error, and cyber literacy and capability – are major contributors to risk and failure.

3. Five Eyes

New Zealand has strong relationships with our Five Eyes partners through Police, the Intelligence Community, the CERT network and a number of other agencies. This provides a solid basis for seeking guidance and resources, and to delve into our partners' experiences when considering what good practice and a well-functioning operating model might look like. In recent years Australia (Australian Cyber Security Centre), Canada (Canadian Centre for Cyber Security) and the United Kingdom (National Cyber Security Centre) have all formed a national 'hub' as the central point for cyber security and could represent a useful starting point when considering a single cyber entity for Aotearoa.

4. New Zealand data governance framework has a limited focus

A refreshed Data Strategy and Roadmap for Aotearoa NZ, commissioned by the Government Chief Data Steward, was published by Stats NZ in September 2021. The effect of this and its application to the private sector is unclear. Further, the content does not appear to reflect iwi and Māori data governance and data sovereignty inputs.

Presently, New Zealand's GDPR adequacy finding is currently being re-validated and assessed, in light of GDPR and our most recent update of the Privacy Act. There is an opportunity outside of CSAC's mandate to strengthen our nation's data governance frameworks and regulations through this work, particularly alongside iwi and Māori. While outside our mandate, it is not clear to CSAC that GDPR responses in Aotearoa have given sufficient consideration to Māori data governance and data sovereignty concerns.

Appendix 2 : Iwi and Māori Considerations of Cyber Security, Data Governance, Data Sovereignty and Cultural Capital

Recent developments

Engagements between the National Iwi Leaders Forum (NICF), the Data Iwi Leaders Group (Data ILG), Te Kāhui Raraunga (TKR) as the operational arm of the Data ILG and the Government (on behalf of the Crown) has resulted in two Mana Ōrite Agreements with the Government Chief Digital Officer and Statistics NZ and the Department of Internal Affairs in recent years. The Mana Ōrite agreements sit alongside the Data and Strategy Roadmap for Aotearoa New Zealand with a focus on areas of priority for iwi and Māori in ensuring Te Tiriti is upheld with respect to tino rangatiratanga, ōritetanga, active protection, options and partnership. Our investigations indicate that these agreements represent significant work programmes and TKR has appointed technicians to work alongside Stats NZ and DIA respectively. With the scale of these work programmes, there is not a strong focus on cyber security capability and resilience.

Tikanga in Technology – Indigenous approaches to transforming data ecosystem is an MBIE Endeavour funded four-year project (2021-24). It seeks to test Māori approaches to collective privacy, benefit and governance in a digital environment with a view to increase the benefits to Māori and reduce data harms. It focuses on two key questions; i) how tikanga Māori (customary protocols) and Mātauranga Māori (Indigenous knowledge) can inform the construction of digital identities and create a better understanding of relational responsibilities to data and ii) what tools, processes, and mechanisms create transformative ecosystems for indigenous data that enable ethical use and generate equitable benefits. A key output of this research includes the development of a Māori Data Privacy Framework.

A more inclusive framework

Consideration of Te Tiriti o Waitangi/The Treaty of Waitangi, the UN Declaration on the Rights of Indigenous Peoples and of tikanga Māori guiding legal and policy will be required to create an inclusive framework that makes sense to iwi and Māori business. Te Ao Māori perspectives of individual versus collective ownership of some data, such as DNA or photos of tā moko, along with consideration of data sovereignty differ greatly from the Pākehā view. An inclusive framework should represent both Māori and Pākehā views. There is little evidence that this has been considered within system strengthening undertaken by Five Eyes partners.

Te Kāhui Raraunga (TKR) was established in 2019, informed by significant work undertaken by the National Iwi Chairs' Forum Data Iwi Leaders Group. This framework is mandated to represent over 75 iwi and hapū, considering such matters as iwi data needs and Māori data governance. Engagement with TKR and informed by the Tikanga and Technology research project would be a good place to start on a reimagined data governance framework for New Zealand and could be a key enabler of strong cyber resilience. CSAC understands the existing mana ōrite agreements with TKR, Stats NZ and DIA are appropriate to explore this further.

Data protection and cultural capital

In giving effect to Te Tiriti, adaptation of a common high-level framework such as the NIST Five Functions might present a useful means of incorporating te iwi Māori perspectives, both in terms of practical guidelines for data discovery in the 'identify' phase, along with specific actions within each function. It is vital that Māori are engaged as partners in the development of any New Zealand interpretation of data protection rules and CSAC sees this as an opportunity for New Zealand to lead the world in data protection, sovereignty and governance oversight, uniquely informed by a Te Ao Māori perspective.

In Te Ohanga 2018, the Māori context of wellbeing extends on the four capitals (natural, human, social, financial/physical) as defined by Treasury Living Standards Framework to include cultural capital. Cultural

capital includes the unique identities of whānau, hapū and iwi, expressed through their different tikanga, kawa, mātauranga, dialects, and whakapapa and are not easily measured by Eurocentric frameworks.

Our investigations indicate that cyber event reporting typically measures financial impact and loss. But for iwi and Māori, loss of cultural capital is equally (if not more so) important. In this respect, cyber security capability and resilience frameworks ought to be more expansive in understanding impact and loss – across all 'capitals', including cultural capital.

Cyber security awareness

Turning our attention to iwi, Māori and Māori organisations, there appears to be little in the way of cyber security awareness campaigns or capability and resilience building targeting these groups. Offerings are generic, targeting the private sector at large such as through the Digital Boost and the CERT/Netsafe campaigns. And as noted elsewhere, we are not convinced of the effectiveness of awareness campaigns even if they were targeted.

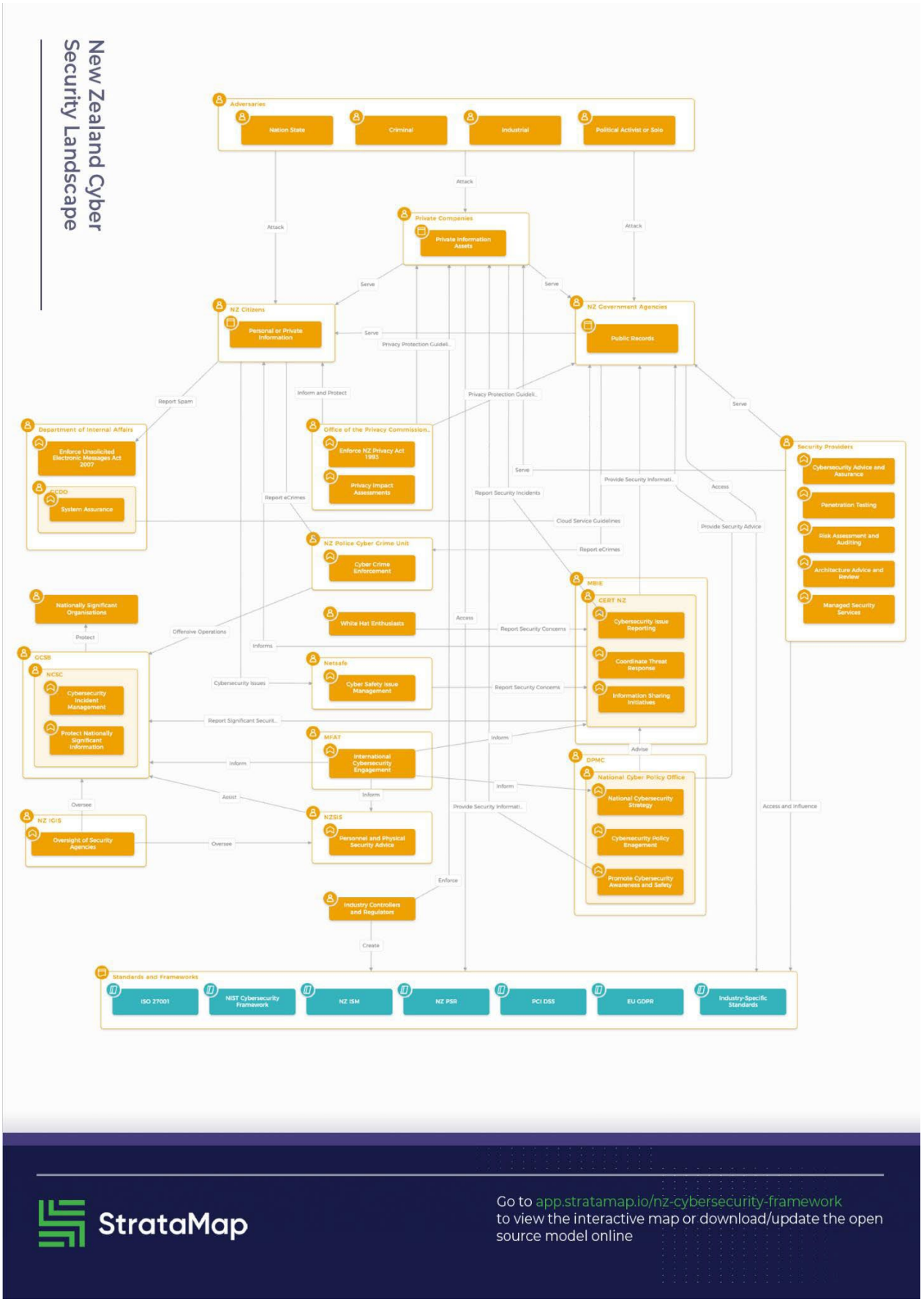
National Iwi Chairs, Te Taumata, the Federation of Māori Authorities, Regional Māori Business Networks, Māori business specific networks and the emergence of Amotai as a leader in supplier diversity and social procurement across Aotearoa all provide avenues to reach into hapori and pakihi Māori. These groups exist alongside Chambers of Commerce and sector groups such as the EMA and are key connectors in a reimagining of a single front door approach.

Sentiment analysis from leaders in the Māori sector representing iwi, finance, banking, education, agriculture, health and ICT indicates that awareness and understanding of cyber risk is immature. Organisational preparedness reflects this, which is of note given that external threats are increasingly savvy (such as phishing in te reo Māori). This was also evidenced in the survey experience of workstream 3.

Next steps

CSAC recommends the creation of a separate workstream comprising the appropriate experts to consider specific inclusion of Te Ao Māori into national cyber standards for data governance. This stream would also look at ways to lift cyber security awareness in the Māori sector. We recommend that this workstream be driven outside of CSAC, given it is broader than cyber security and falls outside of our ToR.

Appendix 3 : New Zealand Cyber Security Landscape



Appendix 4 : Change exemplars: HSWA, Privacy, Electricity and Environmental oversight

1. HSWA and Privacy Act 2020 shifted the dial

The introduction of the Health and Safety at Work Act 2015 (HSWA) and the Privacy Act 2020 (Privacy Act) provide exemplars of introducing legislation and guidelines that have shifted performance, while creating clear rules and expectations for New Zealand enterprises and agencies. It is noteworthy that both pieces of legislation:

- provide fewer prescriptive and mandatory requirements than they do practical tests of reasonableness – specifically steps that are 'reasonably practicable' in the case of the HSWA, or aligned to the provided information privacy principles in the case of the Privacy Act (albeit with highly prescriptive requirements for notification);
- were drafted with close consideration of equivalent legislation in Australia, given the trading relationships between both countries and the significant number of New Zealand organisations with operations of substance in Australia; and
- fail to give effect to Te Tiriti o Waitangi.

2. Guidelines v prescriptive standards

Generally-accepted good practice sees most businesses operating under some form of risk management framework, be it a comprehensive enterprise risk management framework for a larger organisation, or a simple risk register for smaller businesses. Insurance company and supply chain expectations for evidence of some form of working risk management approach has seen terms such as critical risk, risk mitigation and continuous oversight broadly enter the lexicon of business since the 1990s.

CSAC contemplated the use of guidelines or prescriptive standards for compliance as an effective tool to raise New Zealand's cyber defences. In considering such comprehensive frameworks as, say, ISO27001 for cyber risk management, consideration was taken of H&S expectations and how these had been so clearly defined. Using occupational health and safety as an example, the ISO 45000 family (H&S) and the ISO 31000 family (risk management) provide useful tools for developing dynamic risk management frameworks, but the HSWA sets out only minimum legal expectations and breach consequences. Guidelines such as those with the NZ Institute of Directors' Health and Safety Governance and the EMA's Health and Safety at Work guides form a proxy standard against which reasonable and prudent actions might be measured. That is, the HSWA issues few mandatory requirements for compliance (reporting and staff consultation being the main two); the effect of the Act is given through guidelines for behaviour that is reasonable and 'practicable'.

Given the goal of creating a controls framework for improvement for all New Zealand companies and organisations, CSAC recommends that guidelines, not prescriptive practice standards, form the basis of any cyber defence legislation.

Appendix 5 : Australian Security Legislation changes

Source: Lexology.com, 6 February 2022

The Australian Federal Government's recently released Security Legislation Amendment (Critical Infrastructure) Act 2021 (Cth) (SOCI Act) has amended the Security of Critical Infrastructure Act 2018 (Cth) with a view to further managing the complex and evolving national security risks of sabotage, espionage and coercion posed by foreign involvement in Australia's critical infrastructure. The amended SOCI legislation sees an increase in the critical infrastructure asset classes from 4 to 11 sectors, namely communications, data storage or processing, defence, energy, financial services and markets, food and grocery, health care and medical, higher education and research, space technology, transport, water and sewerage.

Importantly, the amendments have increased reporting obligations for critical assets. In the event of an attack on a critical asset, government notification is required. In addition, government assistance and intervention powers have been introduced to allow for an urgent response in situations that present a material risk to national security.

What are the changes to Australia's Critical Infrastructure Laws?

In November 2020, the Parliamentary Joint Committee on Intelligence and Security (PJCIS) recommended two new legislation pieces be passed. However, since that time, the consultation process has seen extensive changes made to Parliament's original proposal. Following the PJCIS recommendations, the original SOCI Bill was split into two amendments, Bill One (the SOCI Bill as passed by Parliament) and Bill Two (there is no timeframe for passing),

Bill One

Bill One expands the coverage of the original Act, by extending the definition of 'Critical Infrastructure Assets' to include sectors not traditionally considered to be infrastructure, including financial services. In addition, Bill One introduces positive security obligations for relevant assets, enhanced cyber security obligations and government assistance powers.

Positive Security Obligations

Part 2 of the existing SOCI Act requires assets covered by the Act to provide ownership and operational information to the Secretary of Home Affairs for the Register of Critical Infrastructure Assets (the Register). Bill One will extend this requirement to the expanded class of critical infrastructure assets where appropriate to develop and maintain a comprehensive picture of national security risks, and apply mitigations where necessary.

The Part 2 definition has been expanded to the following Critical Infrastructure Assets:

- broadcasting
- domain name system
- data storage or processing
- a critical financial market infrastructure asset that is a payment system
- food and grocery
- hospital
- freight infrastructure
- freight services
- public transport
- liquid fuel
- energy market operator

- electricity (to the extent not already captured)
- gas (to the extent not already captured).

Bill One will also introduce an all-hazards positive security obligation for a range of critical infrastructure assets across critical sectors. The obligations to be included in the SOCI Act in relation to a critical infrastructure risk management program will be supported by specific requirements which will be prescribed in rules.

The positive security obligations involve three elements:

- adopting and maintaining an all-hazards critical infrastructure risk management program (Part 2A);
- mandatory reporting of serious cyber security incidents to the Australian Signals Directorate (ASD) (Part 2B); and
- where required, providing ownership and operational information to the Register of Critical Infrastructure Assets (Part 2).
- Only the second and third elements of the positive security obligations will be enacted in Bill One (Part 2B & 2).

Part 2B will require owners and operators of critical infrastructure assets to notify the ASD (or other Commonwealth Body notified in the rules) of any cyber security incident that significantly impacts assets. A cyber security incident is defined as one or more acts, events or circumstances involving unauthorised access, modification or impairment of computer data, a computer program or a computer.

The amendment introduces Sections 30BC & 30BD, s30BC is focused on incidents that have a 'significant' impact on the availability of the asset and must be reported within 12 hours, while section s30BD is focused on any relevant impact and must be reported within 72 hours, with non-compliance carrying civil penalties. Section 30BD also applies to incidents that have not yet occurred but will occur imminently.

The legislation is designed in such a way to give the Minister power to 'switch on' and 'off' these obligations. This provides some discretion if, for example, the Minister decided reporting obligations should not apply to one class of assets.

Government Assistance Powers

Bill One will also introduce Part 3A, which grants the Government additional powers enabling them to gather information, take action relating to an incident, and, as a last resort, intervene and take control of an asset when the owning entity is unwilling or unable to resolve a cyber security incident. It is important to note these Ministerial powers can only be exercised if an incident of material risk has occurred, will occur or is occurring and that asset is a critical infrastructure asset.

Entities are primarily responsible for managing cyber security risks through calibrated risk management, preparatory activities and enhanced situational awareness. However, in exceptional circumstances, the enhanced framework will provide the Government with the power to take appropriate steps to prevent and address cyber security incidents that threaten serious prejudice to Australia's interests, mitigate the impacts of such incidents on critical infrastructure, and restore the functioning of those assets. Under the Government Assistance measures, the Minister for Home Affairs to authorise the Secretary of Home Affairs to do one or more of the following:

- Information gathering direction – require the responsible entity for an asset within a critical infrastructure sector to provide information.
- Action direction – require the responsible entity for an asset within a critical infrastructure sector to prevent a cyber security incident, mitigate the impact of the incident, or restore the functionality of a critical infrastructure asset affected by the incident.
- Intervention request – if an entity is not responding to an information gathering direction or an action direction, the Secretary would be able to request assistance from the Australian Signals Directorate through the exercise of intervention request powers about a cyber incident. Essentially, this will be a

last resort power and would also require the agreement of the Minister for Defence and the Prime Minister.

These powers will provide the Government with the power to act in exceptional circumstances to protect our nation's critical infrastructure assets. This will be achieved by enabling the Minister for Home Affairs to authorise the Secretary of Home Affairs to issue an information gathering direction, an action direction or an intervention request.

Bill Two

Critical Infrastructure Management Programme

Bill Two will introduce the first element of the positive security obligation, Part 2A, which will require critical infrastructure assets to develop and comply with a critical infrastructure risk management program – the first element of the positive security obligations. Responsible entities must comply with, review and update the program and submit an annual report.

Enhanced Cyber Security Obligations

Bill Two will also introduce Part 2C, Enhanced Cyber Security Obligations that apply to a significantly smaller subset of critical infrastructure assets that are crucial to the nation, by virtue of their interdependencies across sectors and consequences of cascading disruption to other critical infrastructure assets and sectors.

The Enhanced Security Obligations will only apply to assets considered to be of the highest criticality (systems of national significance). These obligations are intended to build upon the existing strong Government-industry partnership and provide the Government with the information and understanding necessary to reduce the risk and potential impacts of significant cyber incidents. It will also assure the Government that assets of the highest criticality are actively safeguarding their assets from cyber vulnerabilities above and beyond their requirements under the Positive Security Obligations. There will be four distinct components of the Enhanced Cyber Security Obligations which will be activated only on request (meaning there is no standing obligation):

- Develop and maintain incident response plans.
- Undertake a scenario-based exercise.
- Conduct a vulnerability assessment.
- Provide access to system information relating to the functioning of a system.

What entities will be systems of national significance will be declared by the Minister under Part 6A that will be introduced in Bill Two.

Bill One received royal assent on 2 December 2021 and came into effect on 3 December 2021.

The timeline for Bill Two is currently unknown.

Appendix 6 : NIST Cybersecurity Framework

The National Institute of Standards and Technology (NIST) developed the Cybersecurity Framework (CSF) in 2013, through a collaboration between public and private sector organisations and individuals. It has since been modified several times. The CSF was originally designed to support improving the sector of Critical Infrastructure however it has been adopted globally by a much wider audience and the principles are relevant to most scenarios. The CSF itself comprises five core 'functions' as illustrated below (left). Those functions each contain between three and six 'categories', illustrated below (right). Those 'categories' in turn each contain a more granular list of 'sub-categories' (not illustrated).

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

The framework has been shown to be useful from Board and Executive level (at the macro 'function' tier) to the technologist and engineering level (at the detailed 'sub-category' tier).

CSAC considers that the NIST CSF could serve as a useful controls framework that agencies could recommend to companies seeking to improve their security posture for the following reasons:

- It is globally recognised and widely used in practice already;
- It is easily understood at all levels, regardless of the technical knowledge of the reader;
- The 'function' level labels give a clear indication of the five core pillars of a robust security programme, relatable to business objectives;
- The 'sub-category' level provides sufficient detail for security and other IT practitioners to apply the controls in their own context; and
- The framework can readily meet the specific data protection objectives of any consuming organisation - including the unique requirements of iwi and Māori concerning protection of the taonga that is Māori data.

For smaller organisations, adherence to or adoption of the CERT Critical Controls will provide a high level of cyber governance without a large administrative impost or investment. CSAC would expect that larger organisations would likely have both NIST CSF-aligned risk controls that would by their nature meet or exceed the minimum standard of the CERT Critical Controls.

Appendix 7 : Recent Cyber Legislation Updates

Country	Legislation/policy	Date	Description
United States	Industrial Control System Cybersecurity (ICS) Initiative	April 2021	A voluntary, collaborative effort between the federal government and the critical infrastructure community. Encourages critical infrastructure operators to deploy or commit to deploy control system cyber security technologies, bolstering the security and resilience of facilities.
	Ransomware Task Force - Stopransomware.gov	July 2021	Enhances coordination and alignment of law enforcement and prosecutorial initiatives combating ransomware. Website established to help private and public organisations access resources to mitigate their ransomware risk.
	CISA Cyber Exercise Act	**Introduced to Senate in** October 2021	Directs the Cybersecurity and Infrastructure Security Agency (CISA) to establish a National Cyber Exercise Program, in order to test U.S. response plans for major cyber incidents. The bill directs CISA to include a set of model exercises — which could be readily used by state and local governments and private sector businesses to test the safety and security of their own critical infrastructure. Additionally, the bill requires CISA to help those entities design, implement, and evaluate the exercises.
	Ransom Disclosure Act	October 2021	Requires ransomware victims (excluding individuals) to disclose information about ransom payments no later than 48 hours after the date of payment, including the amount of ransom demanded and paid, the type of currency used for payment of the ransom, and any known information about the criminal entity.
	Cybersecurity and Cybercrime Act 2021	November 2021	Repeals the Computer Misuse and Cybercrime Act 2003. The updated legislation provides for a National Cybersecurity Committee and a new legal framework to deal with cybercrime.
	Transport Security Administration directive	December 2021	Orders operators of critical rail infrastructure to report cyber security incidents to the CISA within 24 hours. Also directs organizations involved in 'high-risk' freight railroads, passenger rail and rail transit to designate a cyber security coordinator. Operators must also implement a cyber security incident response plan as well as

			complete a cyber security vulnerability assessment.
	Cyber Directive	January 2022	Prescribed by an executive order signed by President Biden in May 2021, the memo authorizes the National Security Agency to issue 'binding operational directives' that oblige operators of national security systems "to take specific actions against known or suspected cyber security threats and vulnerabilities". Also sets out new obligations for federal agencies and timelines for meeting them.
United Kingdom	UK Cyber Security Council	March 2021	An independent body established by the government to lead the development of the cyber workforce and put it on a par with established professions such as engineering.
	Product Security and Telecommunications Infrastructure Bill (PSTI)	November 2021	Requires manufacturers, importers and distributors of digital tech and IoT products to ensure they meet tough new cyber security standards - with heavy fines for those who fail to comply.
	National Cyber Strategy 2022	December 2021	Replaces the 2016 iteration, going beyond cyber 'security' to highlight the role of 'cyberspace' as a key domain for strategic competition, economic development and social fulfilment. Key focus on developing cyber technical capabilities, growing the workforce, supporting innovation and export, strengthening the UK's global influence, and encouraging a whole-of-society approach. The implementation of the strategy has been allocated a £2.6 billion budget.
	Launched consultations on updating the Network and Information Systems (NIS) Regulations	January 2022	The government has launched consultations on amending the NIS Regulations to include mandatory incident reporting, expand the scope of the regulations to cover managed service providers, and to transfer costs incurred by regulators for enforcing the NIS regulations from the taxpayer to the organisations covered by the legislation.
Australia	Australia Cyber Security Strategy	August 2020	$1.67 billion over 10 years. Focuses on critical infrastructure protection, as well as responsibilities for businesses and individuals to protect themselves.
	International Cyber and Critical Technology Engagement Strategy	April 2021	Provides a framework to guide Australia's whole-of-government international engagement across the spectrum of cyber and critical technology

			issues, by setting out actions the country will take to protect and promote its cyber and critical technology interests.
	Ransomware Taskforce	June 2021	Operation Orcus - the Australian Federal Police will lead a coalition of agencies, including Austrac, state and territory police agencies, the Australian Criminal Intelligence Commission, the Australian Cyber Security Centre, industry, and other government partners to combat ransomware.
	Ransomware Action Plan	October 2021	Outlines the capabilities and powers that Australia will use to combat ransomware, proposes legislative reforms, and provides information on where victims can go for help.
	Critical Tech Supply Chain Principles	November 2021	Ten voluntary Principles designed to help governments and businesses to make decisions about suppliers and the transparency of their own products, grouped under three pillars of security-by-design, transparency and autonomy and integrity.
	Amendments to the Security of Critical Infrastructure Act 2018	December 2021	Introduces mandatory incident reporting obligations for operators of critical infrastructure either within 12 hours (for critical cyber security incidents) or 72 hours (for other incidents). Also covers the redefinition of what is considered 'critical infrastructure', which has been updated to include universities, finance and banking, health and the food and grocery sectors, communications, defence industry, energy, and transport.
Singapore	Safer Cyberspace Masterplan	October 2020	Introduces a suite of initiatives aimed at securing Singapore's digital infrastructure, safeguarding cyberspace and changing the attitudes of businesses and the public toward better cyber hygiene. Specific initiatives under the masterplan include the Trustmark Programme, the IoT Labelling Scheme and the Internet Cyber Hygiene Portal.
	IoT Labelling Scheme	October 2020	Businesses can voluntarily apply to have their smart device products rated according to their levels of cyber security provisions, enabling consumers to identify products with better cyber security provisions and make informed decisions. Singapore has since signed a MoU with Finland to mutually recognise each other's cyber security labelling systems.

	Singapore Cyber Security Strategy	October 2021	Focuses on infrastructure resilience, creating a safer cyberspace, international cooperation and workforce/ecosystem development.
	Singapore Cyber Talent	Since 2020	Includes a suite of programmes targeting different groups from secondary and tertiary students to women, mid-career professionals, people leaders and CISOs. The programme aims to encourage people to consider cyber security as a career, upskill existing professionals, and give cyber security a platform as a profession.
Canada	Cybersecurity Initiatives Program	November 2020	Aimed at coordinating and aligning national initiatives to strengthen cyber security capacity across Canada's research and education sector. The government invests in initiatives through the CANARIE network, and applications are managed by a multi-stakeholder Cybersecurity Advisory Committee.
	Ransomware Playbook	November 2021	Contains advice for businesses on how to defend against ransomware and how to recover from an attack.

Appendix 8 : Clarifying the Insurance Landscape

There is significant under-insurance in New Zealand in respect of cyber insurance. We understand 6% of businesses held cyber security insurance in 2017. The insurance industry encounters large amounts of apathy from SMEs around cyber insurance. Many SMEs feel they are 'bulletproof'.

Part of the problem for SMEs may be the insurance broker model. Often a broker is pitching an SME a package which comprises risks such as business continuity and fire, among others. Cyber is added as an additional component and the Insurance Council suggests that, with a limited appreciation of the risks, SMEs can feel like the broker is simply trying to upsell them to another product to increase their commission. Broker understanding of the cyber insurance space appears limited and it is unclear whether insurance companies are adequately upskilling brokers on the detail of the policies they are selling.

A recent report from Deloitte made clear the broader challenges in this space. From the perspective of insurers there is a dearth of data, combined with the rapid evolution of cyber-attacks and potential catastrophic accumulation of risk. From a customer's perspective, buyers do not understand risks and options, cyber risk ends up being spread across a range of coverages and the legal/claim landscape is still in flux. Few companies know anyone who has successfully claimed on cyber insurance and there appears to be cynicism from buyers of insurance that any claims will be successfully paid on.

The escalation of premiums is also an issue. Our investigations came across instances of premium/sum insured ratios of less than 1:10, where companies were paying over $100,000 of premium for less than $1 million of possible pay-out (before excess).

Overall, our findings are that the insurance space is confusing and poorly oriented for providing practical help to businesses. We note that Lloyds of London recently indicated they will no longer offer cyber insurance that involves state-sponsored actors. This previously happened in the wake of the NotPetya attacks. Zurich Insurance Group refused to pay out on cyber insurance payments for damages to Mondelez after the NotPetya attack was found to be connected to Russian interests and seen as part of a "cyber war". Given it is not uncommon for states to employ contracted cyber criminals for selected activities, this is likely to further blur coverage understanding.

We note also a recent report from Reuters saying that globally insurers have halved the amount of cyber cover they provide to customers after the pandemic and home-working drove a surge in ransomware attacks that left them smarting from hefty pay-outs.

Taken in its entirety, it is clear that insurance is an important matter for further consideration. It is in the interests of government that the private sector adequately insures itself across a range of existential risks, including cyber. However, the level and cost of cover and the reasonableness of insurers in responding to claims must be understood to be adequately overseen by the market regulator. A review of cyber insurance led by the Reserve Bank would be a useful starting point.

Appendix 9 : Learnings from Privacy

Under the Privacy Act 2020, if an organisation or business has a privacy breach that either has caused or is likely to cause anyone serious harm, it must notify the Privacy Commissioner and any affected people as soon as practicable.

Since its inception (1 December 2020), the mandatory breach notification scheme has generated some unique insights which merit further contemplation, as outlined below:

- Serious harm privacy breach does not necessarily mean "every" instance of a privacy breach
- "Harm" extends to reputational, emotional harm, including identity theft
- "As soon as practicable" for some sectors may trigger transnational compliance and regulatory activity outside New Zealand
- Data privacy maturity in general is lacking in New Zealand
- Internal recording of near misses of breach events is good practice
- Reported serious harm privacy breaches is due mainly to human error versus malicious attacks
- Queries to the Office of the Privacy Commissioner (OPC) suggest that the private sector is starting to mobilise around Data Privacy (for the better).

Our view is that if a mandatory reporting system were to be introduced, it should take into consideration the current mandatory breach notification scheme per the Privacy Act 2020, the gains it has made since inception and the caution to avoid a two-systems approach. Considerations might include the reporting of a serious harm privacy breach as distinct from the reporting of a serious harm data breach and the reporting of everything else. In a time of heightened cyber-attacks, new legislation to require the mandatory reporting of cybercrime requires further scrutiny.

Pros

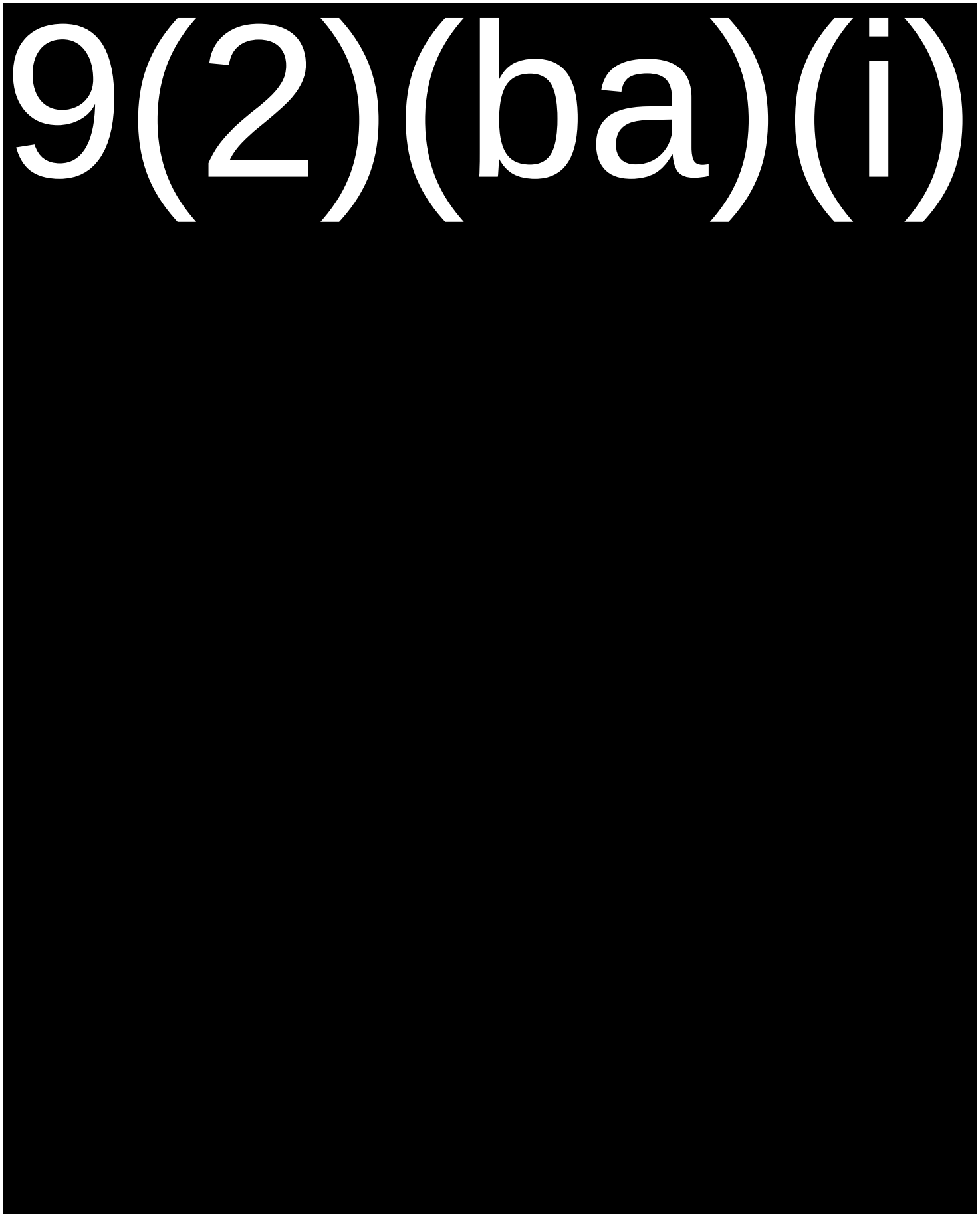
- Consistent with New Zealand's Five Eyes partners
- Consistent with other jurisdictions
- Imposes a cyber security duty of care - similar to Workplace Health and Safety legislation
- Can sit alongside the introduction of an Insurance Levy - similar to EQC or ACC - as incentive to raise resilience.

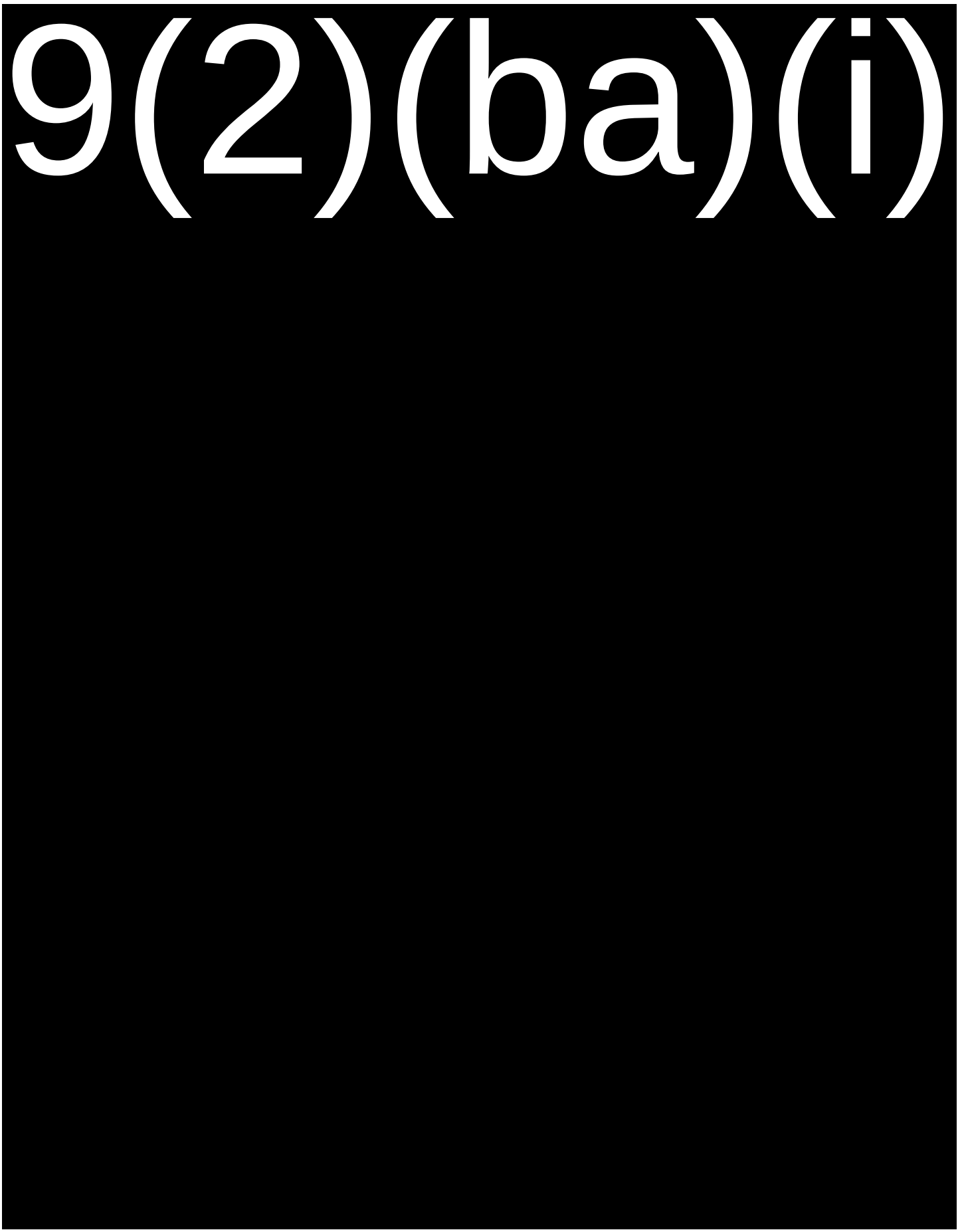
Cons

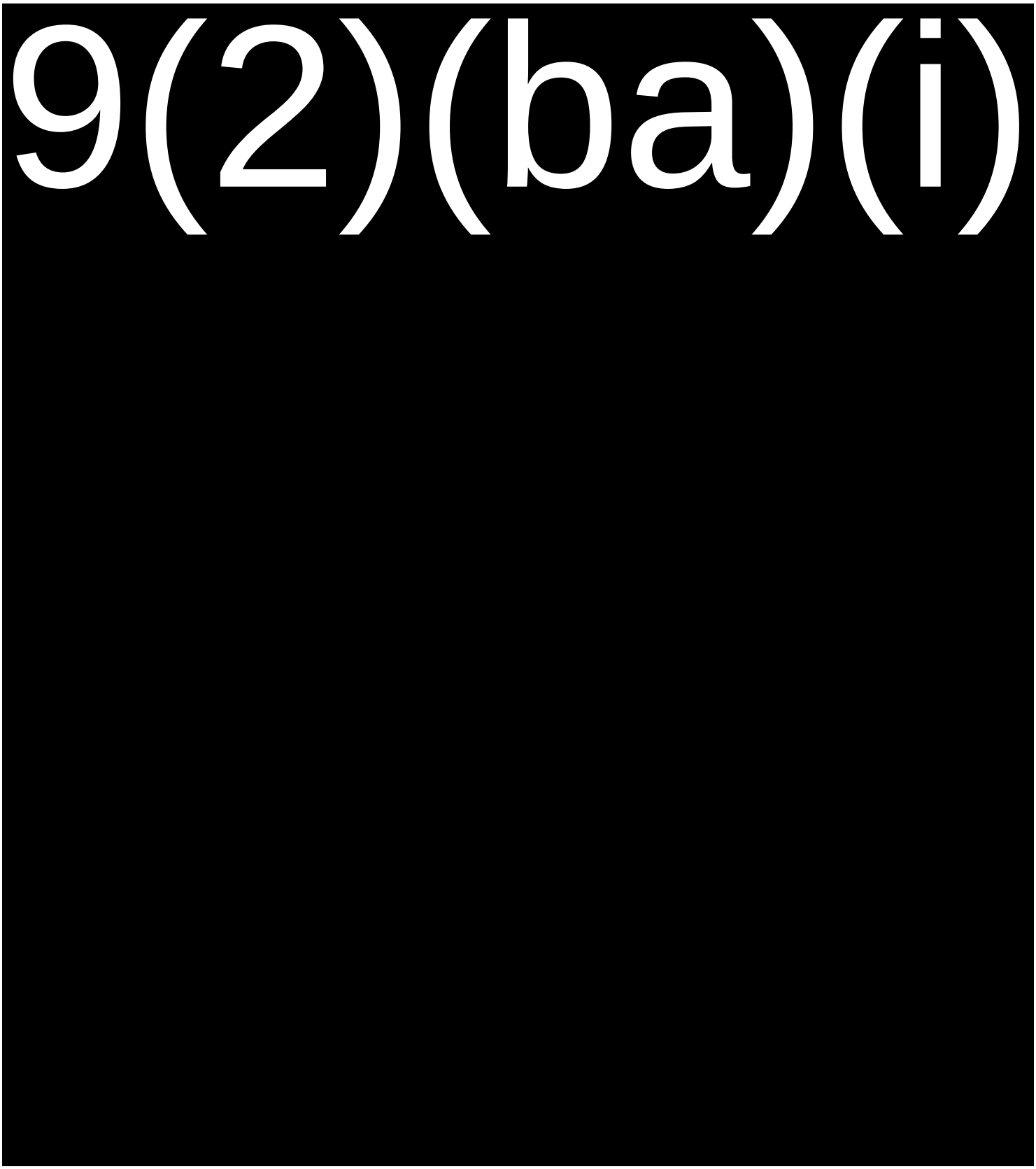
- The time needed to legislate new statute is lengthy and will not yield an "immediate" response to lifting the cyber security capability of the private sector and its resilience when under threat
- Public sentiment and appetite to mandates in the context of the Government's response to COVID-19 pandemic
- May constrain or erode the building trust and confidence across public sector agencies.

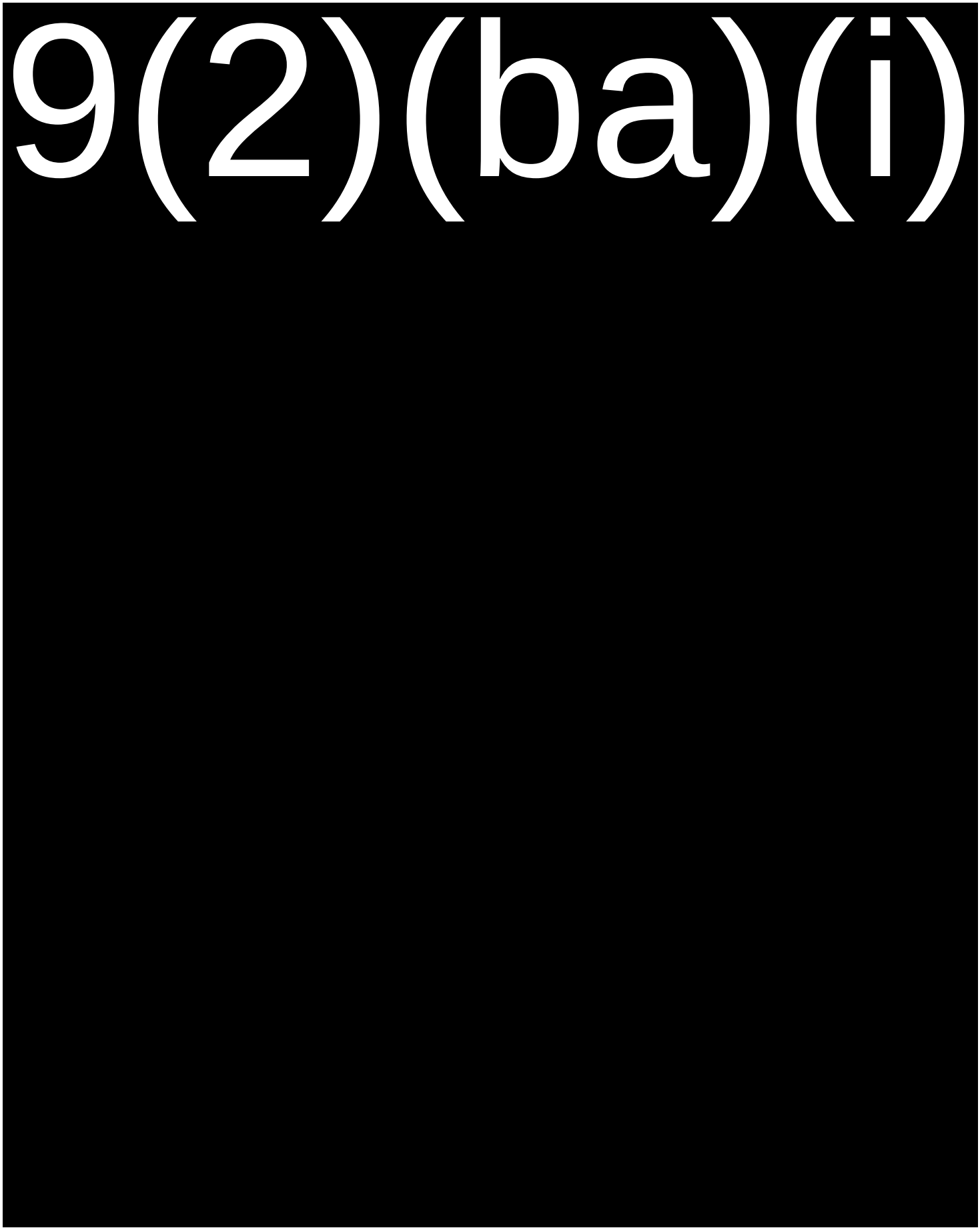
If we are to move to some sort of mandatory reporting we believe it makes sense to have an interconnected regime with the Privacy Act and OPC, which might mandate cyber security incident reporting (over a certain threshold). We suggest any new regime seek to operationalise a duty of care on business or boards over a certain size (drawing on the workplace health & safety model) and consider enforcement powers for appropriate agency or agencies.

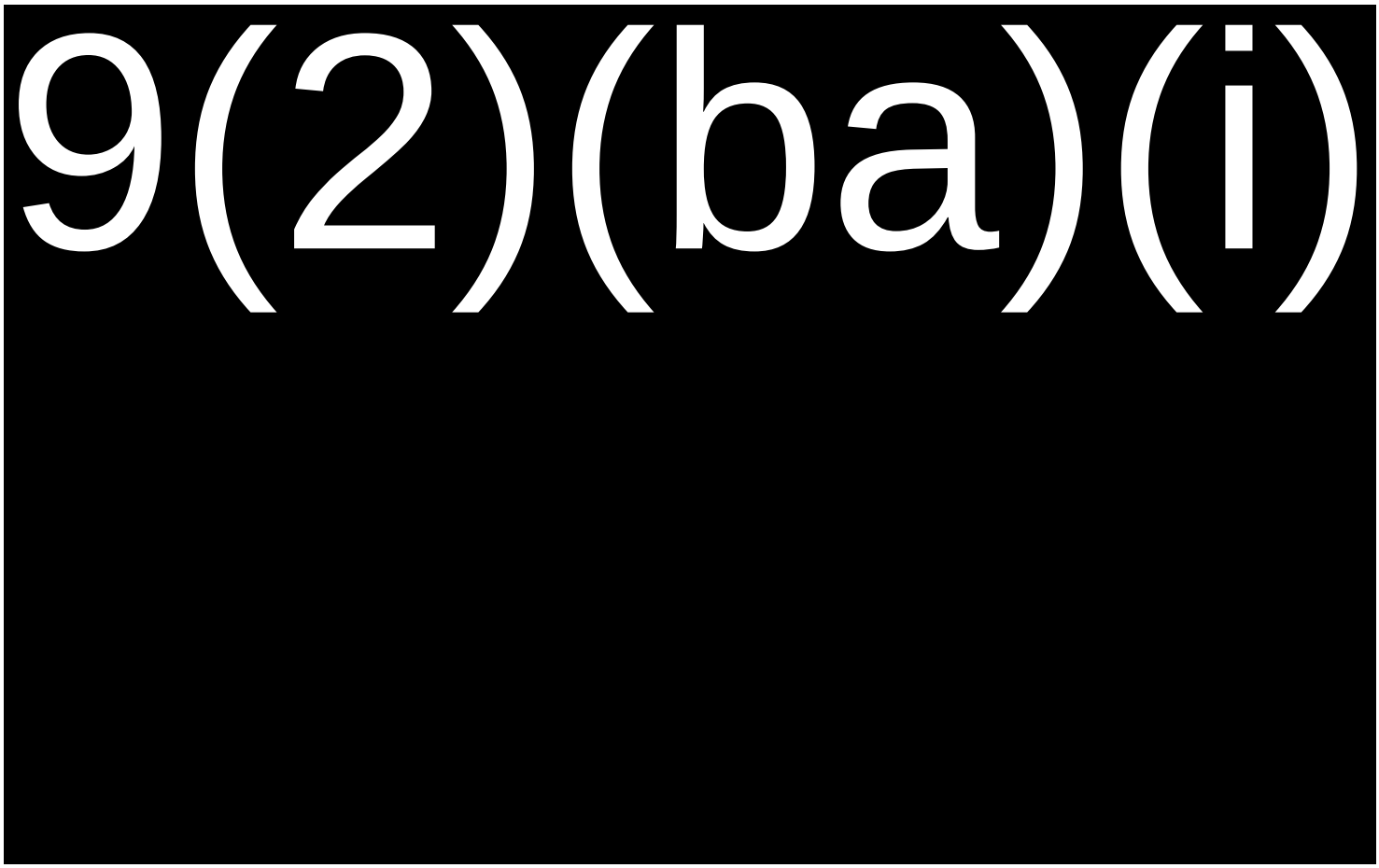
Appendix 10, pages 29 - 33 are withheld in full under s9(2)(ba)(i)


9(2)(ba)(i)


9(2)(ba)(i)


9(2)(ba)(i)


9(2)(ba)(i)


9(2)(ba)(i)

NZ Cabinet Cyber Security Advisory Committee

Proposal on Cyber Security Single Front Door

Scope

What's in scope for the single front door?

- All trading entities and enterprises – from sole trader to NZ arm of multinational, Post Settlement Governance Entities, commercial/non profit/charitable, private/public.
- Cyber incidents, cybercrimes (e.g. system compromises, ransomware, data breach, unauthorised system access, etc).

What's out of scope for the single front door?

- By group – NSOs, non-business: individuals, mums and dads.
- By attack vector - HDC victims, image abuse, intimidation, romance scams, individual financial fraud and identity theft.

CSAC timeline

Dec 21 — CSAC formed – 4 terms of reference

Feb 22 — CSAC delivers findings on:
- Capability
- Cyber security framework
- Private collaboration forum

March 22 — CSAC delivers customer orientation study findings

June 22 — CSAC delivers Supplementary Issues paper

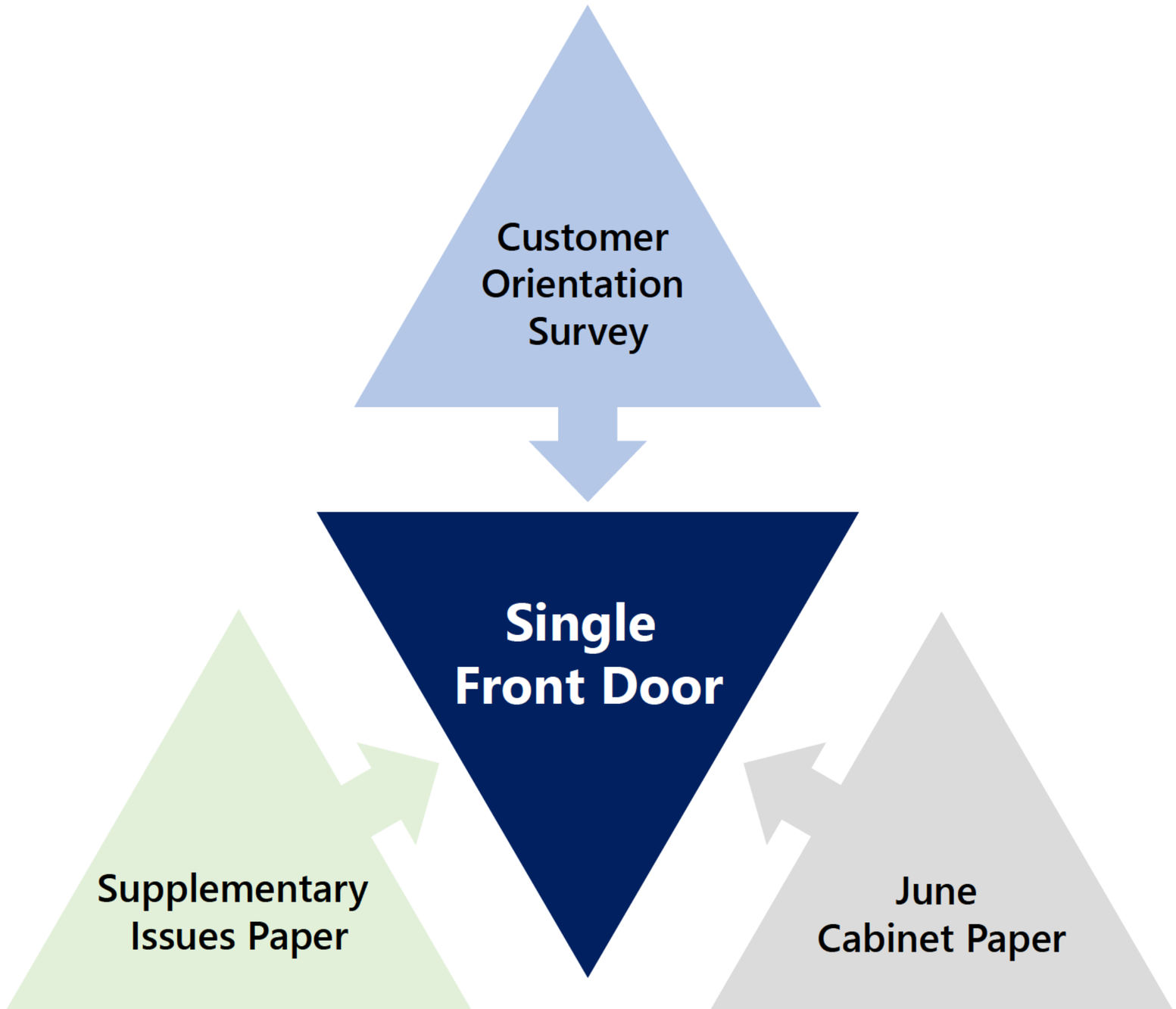
July 22 — CSAC review of June Cabinet paper

Sept 22 — SFD draft to agencies for feedback, gather other insights

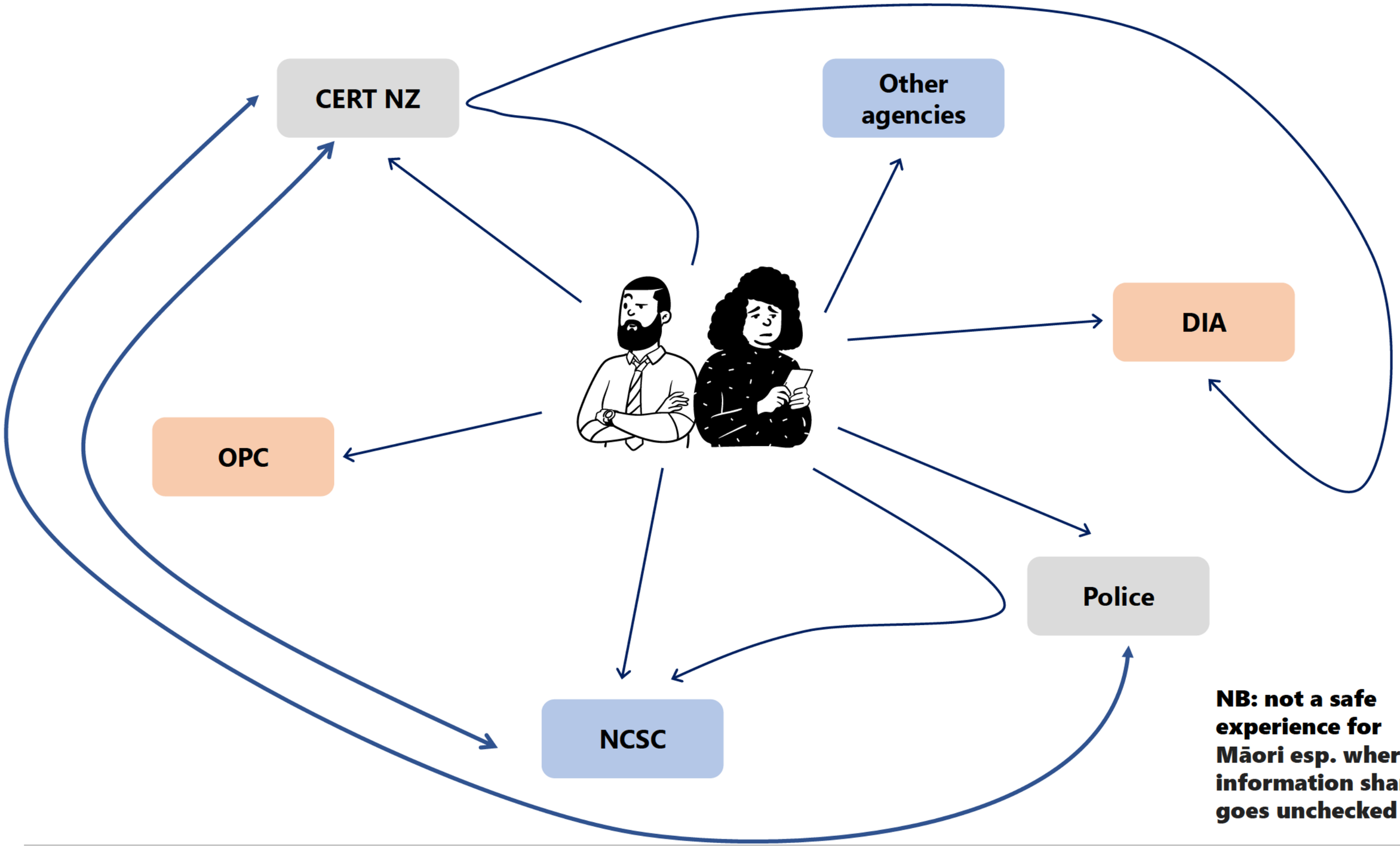
Sept 22 — CSAC finalises SFD proposal

15 Oct 22 — Final SFD recommendations to Ministers

The Single Front Door concept fell out of all workstreams



Current merry-go-round experience for business victims

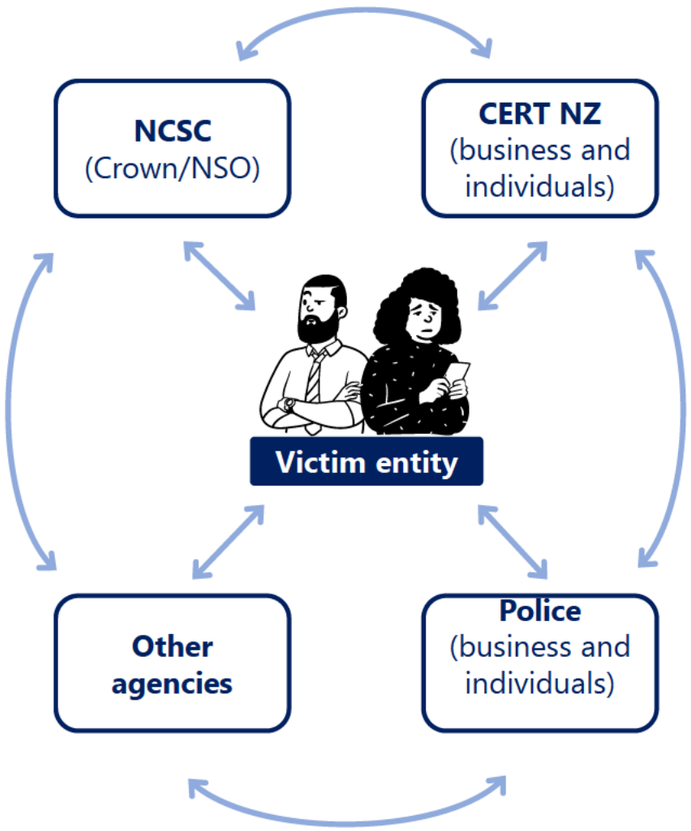


Proposed victim experience: Single Front Door

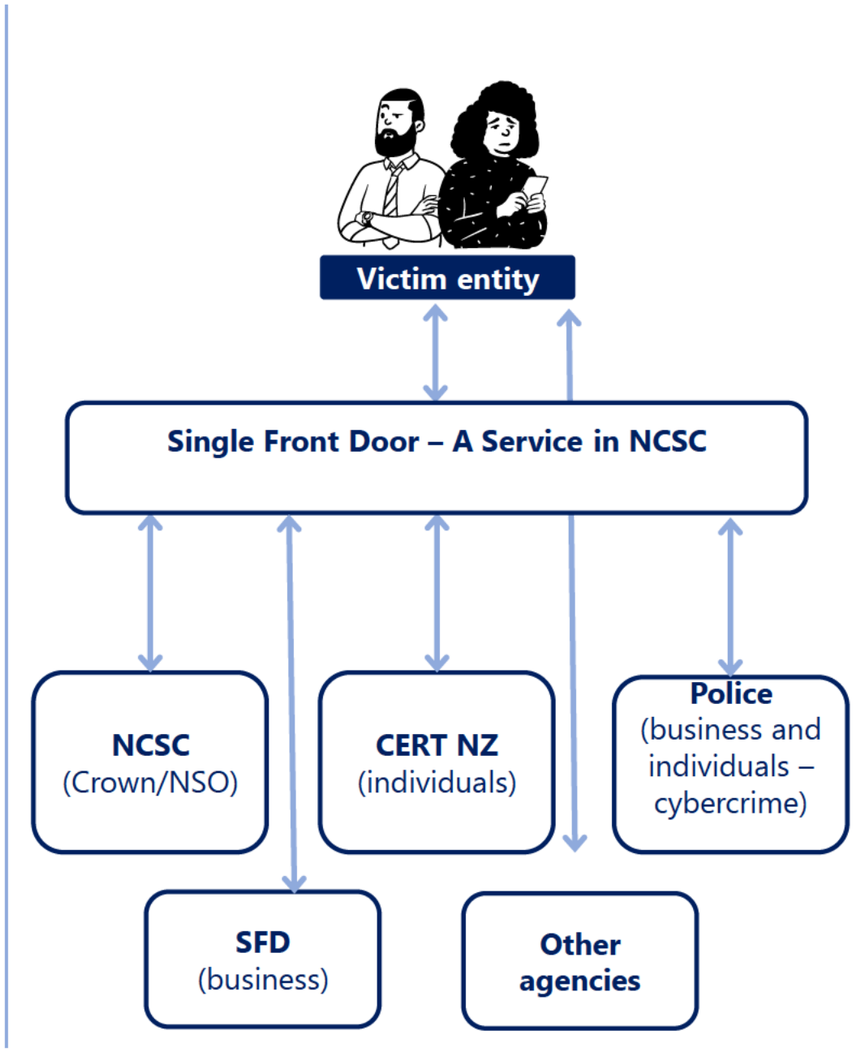
- An alternative to a single agency, when you don't have a single agency.
- The Single Front Door swings both ways …
    - Proactively keeps in touch with the victim AND works with them until affected systems are recovered.
    - Victim centric case management oversight until the case is closed.
- Single Front Door = No Wrong Door
    - If a business makes initial contact via other means (eg Police/NCSC/CERT and in some cases Netsafe), these agencies capture details and share them with SFD.
    - In most cases SFD becomes the victim's case overseer (except police investigations + NSOs) but victim can still deal directly (e.g. for OPC and FMA).
- SFD accountable for triage, shepherding and reporting; also provides incident reporting rates by sector and incident type, case closure rates and victim satisfaction stats to government.
- Provides a single, simple victim reporting portal (similar to ACSC's "Report Cyber") with relevant agency feeds.
- Also worth considering a cyber security minister for policy, strategy and cross government input (as per Australia).

Stepping stone to target future state

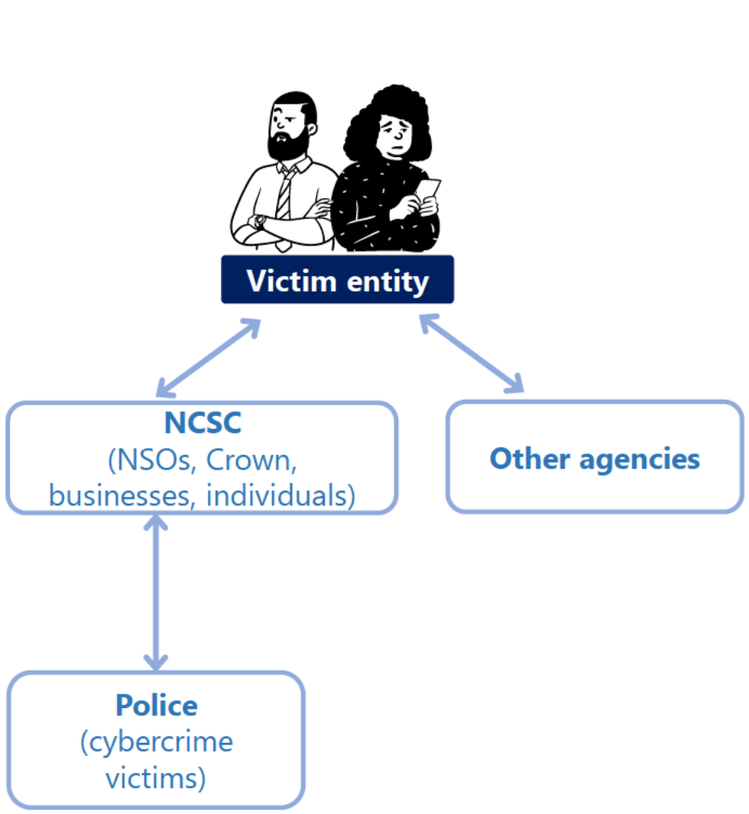
Current victim experience



SFD: interim victim experience



Future victim experience



NB – For SFD and target end state – Te Tiriti will be baked into the triaging and response.

Single Front Door: victim use case insights

CSAC developed five attack use cases (see **Appendix 1**).

These take a user-centric approach to the lifecycle of a cyber attack to capture key points of contact, assistance provided, handover points and expected outcomes.

Key insights were:

- Multiple handoffs are a risk; a single group accountable for oversight of all business cases would add significant value.
- Victims do not know what "box" they fit into and often situations escalate across sectors, software platforms and ecosystems; 'cradle to grave' stewardship will afford best opportunity to act early, warn others and build a shared knowledge base.
- Netsafe has a role to play in some cases, particularly where engagement with social media or hosting providers is required.
- Inter and intra-agency collaboration is paramount – events can require real time responses. Gravitas and mandate will be required to shepherd large and disparate interest groups and maintain oversight even when a significant event is being led by one agency.
- Cultural sensitivity is a must. Cyber security incidents involving Taonga, cultural identity or Te Tiriti implications require specialised triage and victim management. SFD triaging can take lessons from e.g. Whakarongorau NZ Telehealth Services who worked with iwi-affiliates and Māori partners, establishing specialised call centres during the pandemic.

So why have the Single Front Door sitting in NCSC?

1. Consistent with Five Eyes nations; NCSC has deeper connectedness to what's happening in the global and local intelligence environment.
2. NCSC have useful empowering legislation.
3. CERT's position within MBIE creates possible focus and line-of-sight risks (CERT has been funding constrained).
4. NCSC have access to classified and unclassified intelligence, which along with the technical expertise of Five Eyes partners, can put the incident in context.
5. Many of the larger business cyber attacks are from state sponsored actors (or associated with them).
6. Many businesses in the CSAC survey reported NCSC as being useful and practical in supporting them to resolve their problem.

But …

If SFD is to be part of NCSC and sit alongside the existing engagement and outreach division then:

1. NCSC needs substantial new funding (people, platform, process, tools) in addition to any increase associated with merging agencies.
2. CERT is doing good work, has good tools and talent – this should be integrated into the SFD with change oversight driven by what's best for NZ.
3. SFD needs huge cultural orientation change – not trivial for NCSC.
4. NCSC needs to build authentic transparent relationships with iwi + Māori.
5. SFD leader will need proven private sector experience in delighting customers and user centricity.

Minimum viable product: SFD 1.0

What it is:

- A channel for all businesses in Aotearoa when they have experienced a cyber attack + need help to continue to trade.
- A trusted advisor who can help them understand what has happened and what the stages are to fixing it.
- A friendly voice/email to support them as they go about solving their own problems, and help shepherd them through the cyber security incident ecosystem.
- Someone who can save them time and money by providing victim centric information as and when needed.
- A one stop shop for businesses reporting a cyber security attack, the details of which will then be passed on relevant agencies as appropriate.
- A resource with proactive playbooks, training and informed resources. Small enough to be co-ordinated but smart enough to be making world class oversight, handover and response decisions. NB: if resources are in Māori then te reo triage should also be available.
- Harnessing a well-designed and resourced triage process. In particular, seamless referral to Police of relevant incidents is key.

What it isn't:

- An outsourced security service – no "blokes in vans with spanners".
- A substitute for specialist knowledge already within CERT, NCSC, Police, Netsafe or a security consultancy.
- A place to expect the government to fix things for free when businesses haven't taken appropriate security measures (cf: Police attending a burglary. They won't fix your windows or pay to get your door replaced).
- A greenfield project – there is already good work being done we can take forward.

Value add by victim type

For smaller businesses	It helps them understand the attack and provides them with the knowledge and connections to help them resolve it and get trading again.
For larger businesses	It helps them run their own process where the victim will corral a number of specialists (internal and external) who together will confirm the problem, provide advice on resolution, drive the implementation and help get the target business trading normally again. (War room sits at victim end).
For Māori enterprises	The ability to report a cyber security incident with cultural/Te Tiriti ramifications, such that it is fully responded to in an sensitive manner. *NB: Real chance to be a world leader on this as currently no-one does it well (that we have been able to find).*
For individuals	Individuals would have their details recorded and then be redirected to CERT NZ along with those details - i.e. SFD is not replacing CERT for citizens.
For NSOs	NSOs would have their case details recorded and then be redirected to incident response team in NCSC along with those details.
For Police matters	Victims would have their case details recorded and then the case details are redirected as a matter for NZ Police.

Value add by channel

Customers	Channel	**Total addressable market** (approximate)	**Estimated cyber security incidents handled** (per annum)
NSOs + key providers	NCSC	600	500
Businesses	SFD	557,680	680
Individuals	CERT NZ	4 million	7,500
Individuals + schools	Netsafe	4 million	10,000
Victims of cyber and cyber-enabled crime	NZ Police	5 million	Est. 25,000 +
	DIA	5 million	DIA received approximately 892,500 complaints in FY22 *

** n.b. of which 700,000 complaints were in relation to FluBot*

Where to from here?

- There is a significant gap between the current state and a high performance future state for cyber security prevention and defence. This document represents a call for action for investment in change.
- Government will now firm up organisation design, legislative requirements (if any), funding and resourcing of a minimum viable product of a SFD located inside NCSC.
- A key component will be the SFD reporting tool (which will feed to other agencies).
- CSAC members may be available to provide private sector oversight of the process if deemed useful.

Appendices

Appendix 1: Use cases for SFD

Appendix 2: DPMC study questions

Appendix 3: CERT NZ Original/Current Mandate

Appendix 4: Lessons and challenges shared by CERT NZ

Appendix 5: Possible touchpoints between OPC and SFD

Appendix 6: Current government investment

Appendix 1: Use case examples for Single Front Door

Incident happens	First contact /triage	The Fix	Follow-up	System-level activities
	Account management			
Use case 1: Bob's Plumbing (small business) (hijacked credentials, ransom demand to allow banking, CRM and Xero access) **Victim feels:** • Annoyed • Confused • "Don't have time" • "Just want it sorted" **Victim needs:** • To pay bills and staff • To look clients up • To understand what's happening/what to do	**Use case 1: Bob's Plumbing** • Goes to Police first – transferred to SFD (omni-channel – all doors lead to the SFD). • SFD captures incident details once, shares them with Police, CERT + NCSC. • SFD responder providers initial diagnosis.	**Use case 1: Bob's Plumbing** • SFD helps "bucket up" the fix. • Provides playbook covering off: o Reset passwords, set up MFA o Advice on resetting access to SaaS CRM provider o Who to contact and how at victim's bank fraud team. • Bob is responsible to overseeing the fix, but SFD follows up over following days to help shepherd him.	**Use case 1: Bob's Plumbing** • Once resolved, provides email advice on avoiding a 'next time'. • Follow up call two weeks later to see how Bob is tracking and any outstanding issues.	• Works with professional bodies to prevent repeat incidents (e.g. Bankers' Association, NZITF, InternetNZ, NZTech, IT Professionals) • Maintains relationships with national Māori organisations • Analyses metadata from incidents • Embeds Te Tiriti in the triage process. • Broader data sovereignty and data governance considerations.
Use case 2: Aoraki College (medium) (phishing leads to false invoicing + payment) **Victim feels:** • Overwhelmed • Confused • Fish out of water • Concerned about reputation **Victim needs:** • To know what to do • Advice on what to tell the students • Diagnosis of the problem • To stop this from happening again	**Use case 2: Aoraki College** • Contacts via phone. • Capture initial incident details shares details with Police, NCSC and CERT. • SFD responder gives initial prognosis of what has happened.	**Use case 2: Aoraki College** • Refers victim to AoG panel of private security consultants to find a trusted partner to help manage the fix. • SFD provides: o Response checklist/playbook o Comms advice (scripts) for students and public o Connections to previous victims who have experienced the same thing and been through the fix process o Advice on who to contact for insurance and privacy elements (Police, OPC) o An outline of what each of the three core agencies does and works with those agencies on the victim's behalf.	**Use case 2: Aoraki College** • SFD provides follow up calls/emails to check on how fix is going. • SFD determines if its playbooks/checklists need updating in light of learnings from this incident.	
Use case 3: Acme Funds Management (large $10b) (DDoS site takedown with ransom demand) **Victim feels:** • Alarmed/concerned • Unsure what to expect • "Worst nightmare" • "Tempted to pay ransom to buy time to put in proper fix **Victim needs:** • Practical advice • Clarity – can SFD help, if not, who can? • Advanced tech support, gap analysis on response plan • To know if others are experiencing this	**Use case 3: Acme Financial Services** • Contacts via phone. • Capture initial incident details and shares details with Police, NCSC and CERT. • SFD sends confirmation email meeting reporting requirements for the victim to be able to commence cyber insurance claim. • SFD outlines what each of the core agencies does, what help they can provide the victim and acts as the victim's conduit to them.	**Use case 3: Acme Financial Services** • Ideally the victim will put into action an enterprise level cyber incident response plan (IRP) – a case manager will arrange appropriate agency to participate. • If victim does not have a security partner or IRP they are provided details of the AoG panel of private security consultants and playbook around IRP responses. • Connect to others who have experienced the same thing • Advice on who to contact: o OPC o FMA (or other statutory reporting requirements) o ISPs.	**Use case 3: Acme Financial Services** • Give victim transparency on progress of their case – proactive updates by phone. • Once resolved, advice on avoiding a 'next time'. • SFD determines if its playbooks/checklists need updating in light of learnings from this incident.	
Use case 4: Large iwi post-settlement governance entity (large $50b) (phishing leads to loss of tribal whakapapa repository) **Victim feels:** • Responsible • Overwhelmed • Worried • Whakamā **Victim needs:** • To prevent further loss • To secure compromised systems • To make decisions on the ransom • To keep communications limited • To navigate a relationship with Police	**Use case 4: Large iwi post-settlement** • SFD captures incident details once, shares them with Police and CERT. • SFD provides culturally appropriate support (e.g. trigger questions that sees the approach going through a separate triage pathway). • Provides advice on paying a ransom (pros and cons, reality check on likelihood that data will be returned). • Provides an outline of what each of the three core agencies does and works with those agencies on the victim's behalf.	**Use case 4: Large iwi post-settlement** • Victim given playbook on theft of sovereign data. • If victim does not have a security partner they are provided details of the AoG panel of private security consultants. • Advice on who to contact: o TPK o Police.	**Use case 4: Large iwi post-settlement** • SFD provides follow up calls/emails to check on how fix is going. • SFD determines if its playbooks need updating in light of learnings from this incident.	

Appendix 2: DPMC study questions

Q: What would businesses expect in terms of the level of service for incidents of various degrees of impact/severity?

A: We would expect a standard service of 7am-7pm, 5 days a week, with an afterhours service for more serious cyber security incidents.

Q: Would there be a categorisation/prioritisation of some kind?

A: Absolutely. We would need a point scoring system similar to that used by the ACSC that plots size of organisation along with intensity of attack (nature of org could also be a factor).

Q: What would businesses expect in terms of online interaction with the SFD?

A: They would expect to hear back from a SFD triage officer within an appropriately rapid response time – via email or on the phone.

Q: What role does the CSAC see for a SFD in supporting individual victims of cyber security incidents?

A: The SFD will not provide support for private individuals but would capture details and hand them across to CERT.

Q: What role does the CSAC see for a SFD around cybercrime victims?

A: The SFD will take the details of the victim and the crime and pass them to Police (as CERT does also).

Q: What is a typical customer experience look like for a victim business contacting SFD? (Indicatively – we are at the start of the process).

A:
1. A bespoke response/phone or email within as little as 1 business hour according to the severity of the event.
2. An initial diagnosis of what has happened to the victim and an overview of what the fix might include.
3. Victim provided with a list of AoG approved private sector cyber security companies if needed.
4. Victim given a playbook (and other material) relevant to their situation.
5. Having the SFD outline the government agencies the victim may need to deal with (including FMA or OPC responsibilities).
6. Providing targeted introductions to private sector providers – ISPs, MSPs, Bank Fraud, Netsafe, etc.
8. A follow up call back within two days later to check on progress (and further calls as needed).
9. A NPS assessment once they have returned to BAU.

Appendix 3: CERT NZ Mandate

The mandate of CERT NZ in 2022 remains the same as when they were established under the National Cyber Security Strategy 2015 – this being five fold:

1. **Incident response and triage** – taking reports from individuals and organisations, analyse, triage and on-refer.
2. **Situational awareness and information sharing** – sector based info sharing, vulnerability and threat analysis, receive and analyse data feeds.
3. **Advice and outreach** – provide advice on threats/prevention/mitigation, domestic liaison, data reporting.
4. **International collaboration** – liaison with offshore partners and agencies, international organisation membership.
5. **Co-ordination of serious cyber incidents.**

Appendix 4: Lessons and challenges shared by CERT NZ

1. **It takes time to build trust with agencies.** When CERT NZ was established it was a new player in the cyber security landscape, and this meant that it had to establish new relationships and build trust. We would caution against any approach that introduces new agencies into the system, as our experience is that it will take a while for them to be effective.

2. **"Build it and they will come" only gets you so far.** To be an effective reporting and triage agency, you need to be working hand-in-hand with partner agencies. If you build something you hope others will join up and don't require a commitment from other agencies (e.g. a commitment to remove other reporting channels), there are trade-offs:

    - The public continues to get an inconsistent/confusing experience for longer.
    - The time it takes for agencies to decide whether they will shift to a shared platform, and to undertake the necessary legal scrutiny to do this is significant.
    - We consider that Government needs to indicate a clear direction for agencies to follow.

3. **Set a funding roadmap.** Funding for a minimum viable product and with uncertain demand means that the agency will be in a cycle of trying to be funded to undertake its tasks, which takes resourcing away from delivery.

4. **Set a host agency.** Likewise, establishing an agency without clarity on its host agency beyond the first 1-2 years makes it difficult to plan for the medium to long term, and takes focus away from delivery.

5. **Timeframes for new services need to be informed by operational experience.** The pace at which CERT NZ was established mean that some trade-offs were made around reporting and triage design (e.g. there wasn't time in some areas to innovate or request further clarity from Cabinet). If we want the single front door to be transformational, it needs to have the time to build agencies' support and agreement.

Appendix 5: Possible touchpoints between the OPC and SFD

Should the proposed single front door go ahead, the Office of the Privacy Commissioner (OPC) notes that considerable work will need to be undertaken between the SFD as navigator/service channel, and the OPC. Four likely touch points are:

1. At the time a breach occurs – the SFD should refer the "victim business" to OPC to undertake its mandatory breach notification. Should a business come first to OPC, the business should be referred to the SFD to access specialist technical cyber-security support.
2. Reporting on progress with breach response and mitigation.
3. Individuals who contact the SFD for assistance should be made aware of the fact that they can make a complaint to the OPC if they feel that a business has breached their privacy.
4. "Case closure" – it is likely that what defines "case closure" will be different for the SFD and OPC.

Appendix 6: Current government investment

Cyber Security Agency Operational Budgets		
Agency	*Approximate Baseline*	*Note*
CERT	$13.65m	In addition to this baseline funding, we note CERT received additional future-funding in the most recent budget.
DIA	$10.50m	Total B22/23 Appropriation for Digital Safety (includes other non-CS workstreams such as harmful content, community response; and awareness).
NCSC	?	GCSB funding breakdowns are not available publicly.
Netsafe	$4.06m	Figure obtained from 2020/21 Annual Report – note that around three quarters of this funding is for investigating complaints under the Harmful Digital Communications Act.
Police	$2.5m	Estimate from Police Cybercrime.

Source: Public facing agency documentation