Submission document for improving the critical infrastructure resilience of NZ

(from a cyber security and resilience perspective)

Critical infrastructures – like electricity grids, water systems and telecommunications networks – underpin almost all of Aotearoa New Zealand's economic activity and are essential to New Zealanders' health and wellbeing.

To achieve the following strategic direction:

a. a common definition of what counts as critical infrastructure and a framework for identifying which infrastructures are most critical.

b. a shared understanding among critical infrastructure entities and the government of hazards and threats affecting infrastructure systems.

c. a coordinated approach to managing risks across the infrastructure system which accounts for the growing dependencies and interdependencies within and between infrastructures.

In its response to the Infrastructure Strategy, the New Zealand Government supported Te Waihanga's assessment in full.

This work programme's objective is to enhance the resilience of New Zealand's critical infrastructure system to all hazards and threats, both natural (such as earthquakes and floods) and man-made (such as cyber security incidents and espionage).

This would put us in a better position to:

a. protect New Zealand's wellbeing, by reducing outages that undermine New Zealanders' health and living standards

b. support sustainable and inclusive growth in New Zealand's wellbeing, by enhancing New Zealand's attractiveness to investment and business formation.

The Government recognises, however, that resilience is one of many competing objectives for the infrastructure system. These include efficiency; affordability (given implications for equal access to these services); sustainability; and high levels of competition between critical infrastructure entities. Enhancing resilience can be in tension with these other objectives. Recognising this, the government is committed to working with critical infrastructure owners and operators and the public to identify and deliver the 'socially optimal' level of resilience.

The discussion document quotes are in blue and other feedback is in Italics, Black and Calibri font with sources that are authoritative for validity of feedback.

Feedback : At this point, my humble suggestion is that critical infrastructure includes hospitals, banks, electricity distributors, RBNZ, Stock exchanges such as NZX, Traffic control systems, Building Control systems, Railways, Water supply systems, Airports. Anything without which there is will be a major impact to the country.

Banks : ANZ banking services down for a third day as cyberattack impact continues | Newshub

Cyber attack: Kiwibank customers still having access issues - NZ Herald

Reserve Bank responding to illegal breach of data system - Reserve Bank of New Zealand - Te Pūtea Matua (rbnz.govt.nz) (Central Bank attack)

Post and travel systems : Live: Cyber attack fears - Kiwibank, ANZ, NZ Post, MetService back online after CERT flags cyber attacks - NZ Herald

Railroaded: Govt comes under fire following KiwiRail cyber security breach - Computerworld New Zealand **(KiwiRail)**

Planned Outage from NZ Post and Ongoing Cyber Attacks on ANZ Cause Disruption » Bonded New Zealand

Medical industry : A cyberattack lesson from Waikato DHB - The University of Auckland

Waikato DHB cyber attack 'biggest in New Zealand history' - NZ Herald

Schools (Education industry): Cyber bot believed to be behind dozens of New Zealand school bomb threats - ABC News

Otago, Auckland universities caught up in cyber attack | Stuff.co.nz

Government industry : Cyber attack widens, via third party, affecting government agencies | Stuff.co.nz

Farming (Agriculture) : Farmers are being targeted by cyber-criminals (economist.com)

All these attacks have happened in past three years, barring KiwiRail which was over 6 years ago. I have worked on a few projects and no major assessments have been in place there as well (confidential information) for their crown jewels. At this point is cyber security and resilience still at its peak in New Zealand is a good question to reflect on.

We have many attacks, so is it better to broaden the definition of critical infrastructure and regulate the private sector participants and public sector companies to bring them under NZISM. It is sometimes considered a legal burden and a compliance checklist but having updated security framework will enable a digital first approach to Kiwis.

If there is a cost benefit analysis what is the cost of not accessing money when we need it? Or not having schools, power, and hospitals? Today global risks are with state sponsored attackers. This is not an opinion or discriminatory statement just news that gets reported on:

350 cyber-attacks on NZ in last year, a third by state-sponsored exploitation groups | Stuff.co.nz

Suggestion to include new industries in the definition of critical infrastructure.

The approach of UK to critical infrastructure is Critical infrastructure (or critical national infrastructure (CNI) in the UK) is a term used by governments to describe assets that are essential for the functioning of a society and economy – the infrastructure.

According to the Cybersecurity and Infrastructure Agency – an official arm of the United States Government – there are 16 critical infrastructure sectors whose assets, systems and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.

Whilst this is specific to the US, many countries around the world hold the same or similar sectors as critical to the overall infrastructure of the country. These sectors include:

- *Chemical*

- *Communications*
- *Dams*
- *Emergency Services*
- *Financial Services*
- *Government Facilities*
- *Information Technology*
- *Transportation*
- *Commercial Facilities*
- *Critical Manufacturing*
- *Defence Industrial Base*
- *Energy*
- *Food and Agriculture*
- *Healthcare and Public Health*
- *Nuclear Reactors, Materials, and Waste*
- *Water and Wastewater*

Source : Cyberattacks on critical infrastructure - Cybersecurity - NEC NZ

Emulate the ideas and guidance of other countries such as US and UK.

NZDF fends off cyber-attacks in US exercises | by New Zealand Defence Force | Medium and invest in more research.

The cost of a cyber breach is less than the impact. It can also mean partnering with those countries to deal with state sponsored attacks.

For critical areas consider investing in advanced technologies, today AI plays a major role in cyber security risks this is the bad side of AI, so can an investment in AI enabled security in research be useful 350 cyber-attacks on NZ in last year, a third by state-sponsored exploitation groups | Stuff.co.nz.

Is it better to emulate these investments and share knowledge with trusted countries to defend against state sponsored attackers? Some more suggestions include timely actions in critical infrastructure incidents, having forums where industry members can share threat and NOT vulnerability information. The reason being vulnerabilities can be exploited. Ideas taken from abroad are (after Colonial Pipeline attack):

- *to develop cybersecurity performance goals for critical infrastructure. We expect those standards will assist companies responsible for providing essential services like power, water, and transportation to strengthen their cybersecurity.*
- *a voluntary, collaborative effort between the federal government and the critical infrastructure community to facilitate the deployment of technology and systems that provide threat visibility, indicators, detections, and warnings.*
- *requiring critical infrastructure owners and operators to report cybersecurity incidents, designate a Cybersecurity Coordinator, and conduct a review of their current cybersecurity practices. This second Security Directive will require owners and operators of pipelines that transport hazardous liquids and natural gas to implement a number of urgently needed protections, including:*
- *Implementing specific mitigation measures to protect against ransomware attacks and other known threats to information technology and operational technology systems within prescribed timeframes.*

- *Developing and implementing a cybersecurity contingency and recovery plan.*
- *Conducting an annual cybersecurity architecture design review.*
- *Working on policy review and design review of critical infrastructure systems.*
- *Sharing defence intelligence data with other countries.*
- *Tools that range from "resiliency, hardening, deception, denial, along with defending." The plan also looked across domains and potentially vulnerable capabilities all enabled by AI.*
- *Checking for spies from enemy nations and foreign intelligence threats since there is a lot of migration.*

Sources : *FACT SHEET: Biden Administration Announces Further Actions to Protect U.S. Critical Infrastructure | The White House*

Pentagon mulling new critical infrastructure defines ops plan: VanHerck - Breaking Défense

- *For critical infrastructure concerning nuclear and defence capabilities quite a few countries are not able to respond to threats from enemy nations (Russia) for instance, is not a friendly country for New Zealand. Some of the attacks were anticipated and over a year ago but the threats still exist.*

NZ's Russia sanctions: Retaliation may include cyber-attacks, expert warns | RNZ News

N Korean cyber-attacks affected NZ - report | RNZ News

- *Again, joint investments and partnerships with UK and US, investment in critical research areas can be of help during a recession.*

Sources : Eyeing Russia and China, NORTHCOM head frets over US ability to respond to Arctic threats - Breaking Défense

Resilience should be enhanced at the least cost to businesses, consumers, and government by:

- *using non-regulatory mechanisms (such as information sharing) wherever possible, to better target and prioritise investments in resilience, to deliver optimal improvements for each dollar spent.*

- *taking advantage of existing sector-based regulatory regimes wherever possible, by identifying and filling gaps in the existing regulatory landscape, rather than replacing or usurping them.*

- *developing proposals that build on existing and forthcoming laws (to the extent possible).*

- *ensuring that any new potential regulatory approach is proportionate and dynamic.*

- *It should be able to respond to changing risks, technologies, and consumer preferences, to ensure that legislation does not become rapidly outdated or otherwise no longer fit for purpose.*

- *Investing in design of Energy and IT systems with inbuilt resilience and redundancy/ fault tolerance at a conceptual design phase for critical infrastructure. The technical feasibility and cost need to be assessed.*

Sources: Microgrids for Energy Resilience: A Guide to Conceptual Design and Lessons from Défense Projects (nrel.gov)

The costs of enhancing resilience should, where possible, be paid by those who benefit from those investments.

- *Tax can increase a bit more instead of asking the private sector companies to invest in these technologies if that is alright and partnerships with trusted Commonwealth nation may actually be of help. We got interest rate hike, inflation, recession, and layoffs happening at the same time.*

- *To avoid events such as RBNZ and attacks on banking infrastructure APRA requirements, similar guidelines for banking sector such as FFIEC can be adopted for a more stringent security first approach.*

Source : FFIEC Details How Banks Must Manage Cyber Risk | American Banker

Criterion B: How does the s the option change regulatory burden and regulatory certainty across the community?

- *Feedback: This is a great view, but the losses compared to cost of compliance is higher or lower for the Kiwis than the critical infrastructure providers?*

- *Also for critical infrastructure providers is more compliance a burden or a social expectation.*

- *The Privacy Act has a penalty of 10,000 NZD which is a small portion of a company's profits (Privacy Act | Consumer Protection)*

- *In an emergency situation no hospital or power or access to banks is that agreeable from a digital rights and human ethics perspective.*

- *If secure by design and NZISM becomes compulsory the trusted culture will be more of trust but verify and will it lead to innately strong critical infrastructure which is a long-term investment than a short-term cost?*

- *Now, the ransom payment guidelines have been issued but this is only to reduce a company from being preyed on than anything else.*

Events of Kiwis losing quite a bit of money being reported on a regular basis:

New Zealand cyber incidents, financial losses still high despite drop - CERT NZ report | News hub

Kiwis losing millions more to cyber-attacks - and Cert NZ boss says reported no's are 'tip of the iceberg' - NZ Herald

- *The paper rightly identifies the increase in short term costs, when taxes are increased it helps to follow progressive taxation system and to avoid over burdening the high-income earners consider a roadmap for other areas.*

- *It is prioritising critical areas such as Primary Industries, Defence, Education, Energy, Hospitals than commercial businesses as those which operate for public welfare and are a need will require more focus. It can be a budget proposal and creating funds for future uses as well.*
- *Having published guidance and enabling tailoring these with retainer models for leadership and project execution plays a critical role as well All topics - NCSC.GOV.UK.*

The other part this submission stresses on is the importance of retailers and grocery shoppers, they often use POS systems and have unprotected Wi-Fi which is a high-risk area. This is a basic need since we all need food, milk, and basic facilities.

Brazen cyber-attacks a reminder that Kiwi retailers must rethink cyber security - The Register

'Retailers are a key target': Behind the rise of ransomware attacks - Inside Retail

- *My humble point is these areas need more focus too these are small businesses, and such attacks can have a big impact. In rural areas a hospital, farmer or a shop getting affected can affect more people or even public transport systems, water supply systems, electricity grids being impacted can have a major negative impact and more needs doing here since it is more remote than a city.*

- *In this light, identifying areas of high risk say Christchurch (risk from earthquakes or attacks) and planning for resilience or response is an important move to be considered. For this submission, resilience includes availability of necessities and the digital infrastructure which enables it. The paper does not cover other areas such as crisis resilience plans but a national risk assessment with geologists will be of help as well.*

Source: Sector resilience plans - GOV.UK (www.gov.uk).

The business case for these ideas is a direct quote from the paper:

From a cyber perspective, the Australian Government estimated in 2020 that a four-week interruption to digital infrastructures caused by a significant cyber incident would cost their economy approximately 1.5 per cent of Gross Domestic Product.13 The scale of costs would likely be similar in New Zealand (that is, around $6 billion).

In the light of this adopting some guidance from UK may be of value:

1. *Get management on board.*
2. *Involve your entire organisation.*
3. *Back up your data regularly*
4. *Implement backup solutions.*
5. *Simulate security/crisis incidents.*

Source : Cyber Resilience | NI Cyber Security Centre

The business case for these ideas is a direct quote from the paper:

As climate change and associated weather events intensify, and other risks to infrastructure – such as cyber-attacks – grow, resilience will also become an important economic advantage. Investments in critical infrastructure resilience today will help to attract the business investment we need to support productive, sustainable, and inclusive economic growth tomorrow.

- *Investing in Incident Response Readiness Review, Managing crisis and business continuity plans for mission critical areas is a fundamental need in critical areas in NZ.*
- *Resiliency doesn't mean you can defend against all attacks; it means that if you are compromised, you have a plan in place that lets you recover quickly after a breach and continue to function.*
- *Resiliency requires companies to conduct a technology inventory, identify critical application dependencies and vulnerabilities, and incorporate this information into recovery plans and rebuild targets.*
- *Knowing your infrastructure can help ensure a readily actionable response plan that makes an incident economically recoverable.*
- *The next step is to put in place and rehearse an incident response plan.*
- *Define a communications and command structure to ensure business continuity, with provisions for such contingencies as a ransomware attack that affects multiple sites or the need to conduct crisis management without internet access.*
- *Strategically focusing on critical digital assets and the interactions between them, you can proactively protect your data and control access regardless of the locations of your employees or the devices they use.*
- *A good incident response plan will clearly define who's responsible for which actions during an incident and will capture all procedures and best practices for the response. Without clear responsibilities, you may have a plan that nobody knows how to follow.*
- *The incident response strategy should enable you to escalate and respond rapidly, because time is of the essence to ensure business continuity and comply with regulatory mandates.*
- *That means ensuring your senior management and your board are aware of the strategy, as well as enlisting necessary third parties in advance, including partners, legal teams, incident-response services, and law enforcement.*
- *Every employee from the business staff to IT personnel to executives should adopt a cyber-resilient mindset, which begins with recognizing that they are the first line of defence against threats.*
- *Reinforce the culture with continuous security-awareness training—use gamification to let people experiences the impacts of security policies and reward them for doing the right thing rather than punish them for mistakes.*

- *Don't assume that your organization's prior investments in security controls will keep you safe.*

- *Keep up with the latest attack methods, and continually evaluate the relevance of your existing controls and plans.*

- *Cyber resiliency begins with a well-defined strategy aligned with a project roadmap and lines of accountability. These plans ensure proper execution of the strategy with decision making based on risk management.*

- *As a foundation, organizations should also have a solid cybersecurity architecture that provides guidelines to make sure the right infrastructure and controls are in place while allowing flexibility for technological change.*

- *While no plan is 100% attack-proof, your cyber-resilient culture can minimize distraction, risk, and damage while ensuring that your organization stays focused on its mission-critical strategies.*

Source : *Make Your Organization More Resilient to Cyber Attacks - SPONSOR CONTENT FROM DXC (hbr.org)*

Some ideas for companies to be more resilient and these need to be tailored:

- *Seek advantage in adversity. Don't merely endeavour to mitigate risk or damage or restore what was; rather, aim to create advantage in adversity by effectively adjusting to new realities.*

- *Look forward. In the short run, a crisis many appear tactical and operational, but on longer timescales, new needs and the incapacitation of competitors create opportunities.*

- *Crises can also be the best pretext for accelerating long-term transformational change. One of the key roles for leaders is therefore to shift an organization's time horizons outward.*

- *Take a collaborative, systems view. In stable times, business can be thought of as performance maximization with a given business model in a given context.*

- *Resilience, by contrast, concerns how the relationships between a business's components or between a business and its context change under stress.*

- *It requires systems thinking and systemic solutions, which in turn depend on collaboration among employees, customers, and other stakeholders.*

- *Measure beyond performance. The health of a business is not captured only by measures of value extracted, which tend to be backward-looking.*

- *Measuring flexibility, adaptation, and other components of resilience is critical to building a sustainable business. This can be done quite simply by looking at either benefits or capabilities.*

- *Prize diversity. Resilience depends on being able to generate alternative ways of reacting to situations, which in turn depends on the ability to see things with fresh eyes. Resilient businesses prize cognitive diversity and appreciate the value of variation and divergence.*

- *Change as the default. Alibaba founder Jack Ma sees change, not stability, as the default.*

- *Resilience is less about occasional adjustments under extreme circumstances and more about building organizations and supporting systems predicated on constant change and experimentation.*

- *This is partly to avoid rigidity and partly because iterative incremental adjustment is far less risky than a massive one-shot adjustment.*

Source: *A Guide to Building a More Resilient Business (hbr.org)*

- *More announcements to business (SMBs) to be informed of resilience is a good idea. The business case for it is a direct quote from the discussion document:*

  While insurance and reinsurance can cover some of the risks to specific assets, it cannot cover or compensate individuals for any long-term hardships they experience as an indirect result of an event. Even where insurance does exist, the government has historically had a critical role in reinstating damaged infrastructure and providing disaster relief.

  Shifting the balance of our expenditure away from (largely government-funded) recovery, towards resilience, is also likely to increase equity, both for members of our communities today and on an intergenerational basis. This is because:

  a. the beneficiaries of underinvestment in resilience for each critical infrastructure entity are relatively narrow (shareholders and customers), while all New Zealanders bear the costs of infrastructure failure.

The only beneficiary is the companies which can afford to make mistakes and be in business due to a monopoly. While it is not the fault of a victim it is good to be more well planned and have foresight. Ideally, having slush funds will help in reducing risk by proactively researching on threats and investment areas.

- *lower income New Zealanders who receive a greater share of direct government fiscal support (e.g., through the social welfare system) bear a disproportionate share of the burden of government funds being redirected towards disaster recovery.*

- *on an intergenerational basis, the costs of disaster recovery will be largely (if not entirely) borne by New Zealanders at the time following the event, while current and previous taxpayers, ratepayers, shareholders, and customers may have underinvested in resilience prior to the event.*

Suggestions in current approach

Successive New Zealand Governments have not taken a comprehensive or coordinated approach to critical infrastructure regulation. No single agency has had policy or regulatory responsibility for New Zealand's critical infrastructure system.

- *Can this aspect change with a nation-wide approach with a leadership or parliament support. The Biden and UK administration are case in point, it will help in more targeted and consensual efforts. For risk management the tone at the top is what really matters before it permeates towards grassroots.*

- *Can the National Emergency Management be linked to cyber threat agencies such as CERT NZ, GCSB where needed such as Colonial Pipeline attack?*

- *Enhancing information-sharing requirements between critical infrastructures and government, to support monitoring and planning (for example, reporting of cyber incidents).*

- *This is a great idea, but can it integrate with benchmarks such as NIST, NZISM, ISO and other frameworks the National Emergency Management Bill?*

The business case is a direct quote from the document:

As described in the Defence Assessment 2021, 32 New Zealand faces a substantially more challenging and complex strategic environment than it has for decades. This makes the risks of manmade shocks higher than they have been in a generation.

Risks of particular relevance to New Zealand's critical infrastructures include those, in cyber space, where:

a. between 2019 and 2022 there was a 45% increase in reports of cybercrime, with intelligence estimates pointing to an actual rise of over 80%; and

b. attacks are increasingly motivated by factors other than financial gain, for example, many cyber-attacks are geopolitically motivated and linked to nation state actors, who seek to disrupt essential services.

Geopolitical tensions are not limited to the cyber domain. By virtue of holding large amounts of sensitive information and their integral role in our economy, critical infrastructures are also attractive targets for:

a. espionage (the covert collection of non-publicly available information

b. sabotage (service disruption) c. coercion (the threat of service disruption to extract concessions from critical infrastructure owners and operators).

These risks can arise through foreign states, or proxies working on their behalf, who gain control of, or access to, New Zealand's infrastructures. This may include through:

a. investment and other commercial partnerships (such as joint ventures)

b. the supply of goods and services (such as managed service providers or software vendors, that could extract sensitive information from corrupted or insecure assets)

c. employment

Many governments are also placing new barriers around the use of some imported products and the export of some products36 to respond to concerns that:

- **the purchase and installation of some goods may, in itself, pose risks (e.g., certain IT equipment may allow systems to be remotely accessed or controlled or allow data to be exfiltrated), or facilitate unethical practices (e.g., modern slavery and other human rights abuses)**
- **the sale of some goods (e.g., semiconductors) may aid the military capabilities of states that are perceived to be hostile.**

- ***Feedback:*** *Procurement contracts can be vetted, C&A on critical imported systems and performing vetting of contractors involved in such development is fundamental.*
- *If we adopt PSR guidance for IT/OT infrastructure it is useful and the skillsets to manage Industrial Control System incidents is completely different from normal incidents, so updated playbooks and response mechanisms are required too.*

The direct quotes from the discussion document which are point blank perfect is.

To manage these breakdowns in supply, critical infrastructure owners and operators may have no choice but to adapt their approach to securing critical inputs, likely at higher cost, which will ultimately be at least partly passed on to all New Zealanders through higher service charges. Depending on how product availability changes, it may also adversely affect the stability of the infrastructure system over the long term.

The adoption of new technologies facilitates (among other things) greater automation, better remote monitoring and management, and greater connectivity. This is delivering savings for business and consumers and enhancing productivity and economic growth. For these reasons, their deployment is welcomed and consistent with the Government's broader economic objectives.

However, the adoption of new technologies also creates new vulnerabilities and stresses by: a. changing what we consider to be critical infrastructure, leaving regulatory systems out of date. For example, as the New Zealand economy becomes more digitised, the service providers that underpin that transformation (e.g., cloud service and data storage providers) will become increasingly critical to the economy's day-to-day function.

However, these service providers are not currently subject to regulations to support or enhance their resilience.

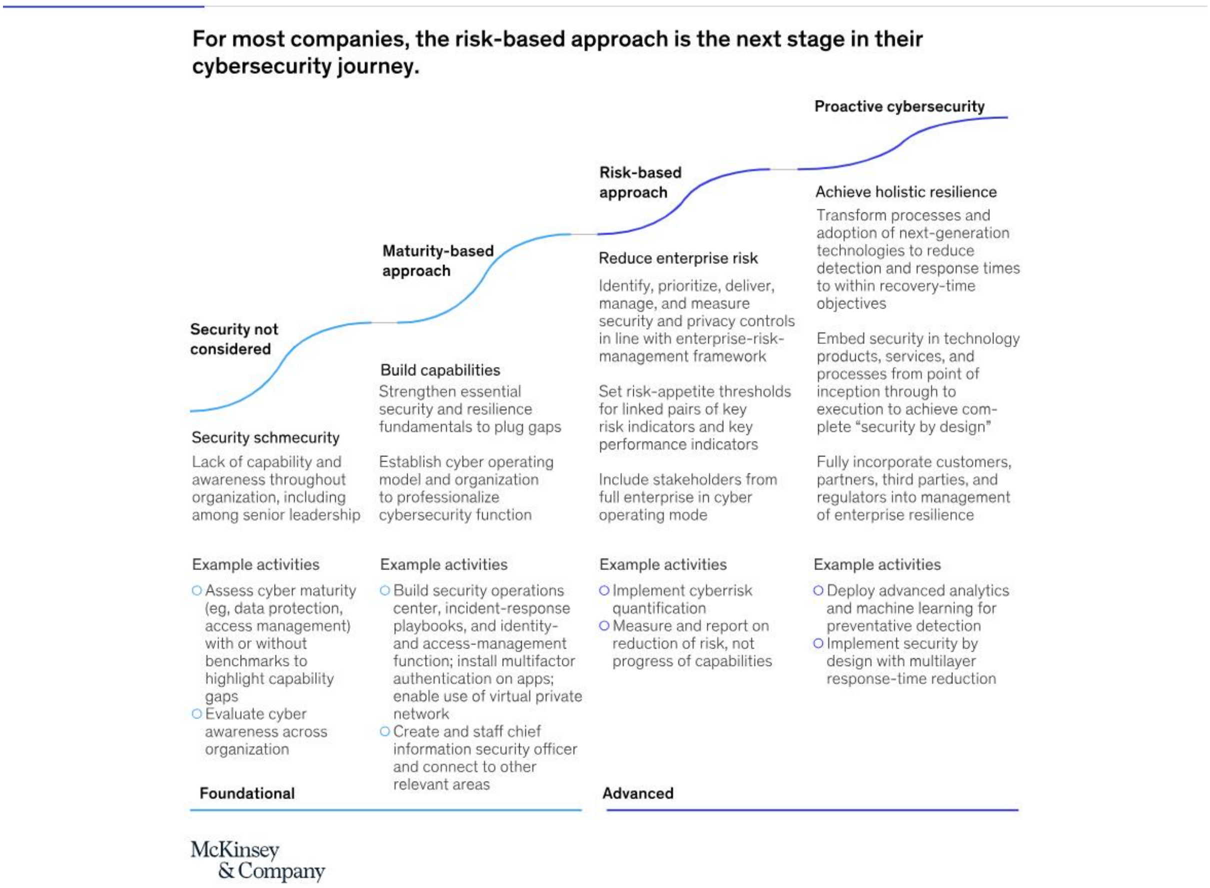
b. introducing new vulnerabilities. For example, technological innovation is driving physical and digital systems to converge (e.g., operational technology (OT) systems are now integrated with information technology (IT) systems such that physical events can be controlled through digital systems connected to the internet).

This creates new challenges to infrastructure resilience – it expands the attack surface and enables malicious actors to gain access to the systems that monitor and control physical equipment, and ultimately disable or disrupt operations.

Feedback: Investing in OT/Industrial Control systems resilience and threat modelling could be a great proactive solution. Its incudes calculating cyber-VAR for high probable threats and simulating losses, and considering recovery from updated Incident Response Plans, insurance etc.

New Zealand's long-standing approach to regulating for critical infrastructure resilience has relied on the assumption that critical infrastructure owners and operators (or regulators) could accurately determine:
a. the likelihood of a shock occurring.
b. knows who or what would be affected by that shock.
c. estimates a shock's costs.
d. makes rational choices about what investments to make to reduce those costs.

Feedback: Resilience is about risk assessment in different areas. A national wide risk assessment plan such as UK for high-risk digital systems could be a great approach. Not having subjective estimates, considering costs from intangible aspects such as perceptions, loss of potential revenue will be of great help. I am quoting a McKinsey resource here since the government is quite proactive which is commendable.



For most companies, the risk-based approach is the next stage in their cybersecurity journey.

Security not considered

Security schmecurity

Lack of capability and awareness throughout organization, including among senior leadership

Example activities

- ○ Assess cyber maturity (eg, data protection, access management) with or without benchmarks to highlight capability gaps
- ○ Evaluate cyber awareness across organization

Maturity-based approach

Build capabilities

Strengthen essential security and resilience fundamentals to plug gaps

Establish cyber operating model and organization to professionalize cybersecurity function

Example activities

- ○ Build security operations center, incident-response playbooks, and identity- and access-management function; install multifactor authentication on apps; enable use of virtual private network
- ○ Create and staff chief information security officer and connect to other relevant areas

Foundational

Risk-based approach

Reduce enterprise risk

Identify, prioritize, deliver, manage, and measure security and privacy controls in line with enterprise-risk-management framework

Set risk-appetite thresholds for linked pairs of key risk indicators and key performance indicators

Include stakeholders from full enterprise in cyber operating mode

Example activities

- ○ Implement cyberrisk quantification
- ○ Measure and report on reduction of risk, not progress of capabilities

Proactive cybersecurity

Achieve holistic resilience

Transform processes and adoption of next-generation technologies to reduce detection and response times to within recovery-time objectives

Embed security in technology products, services, and processes from point of inception through to execution to achieve complete "security by design"

Fully incorporate customers, partners, third parties, and regulators into management of enterprise resilience

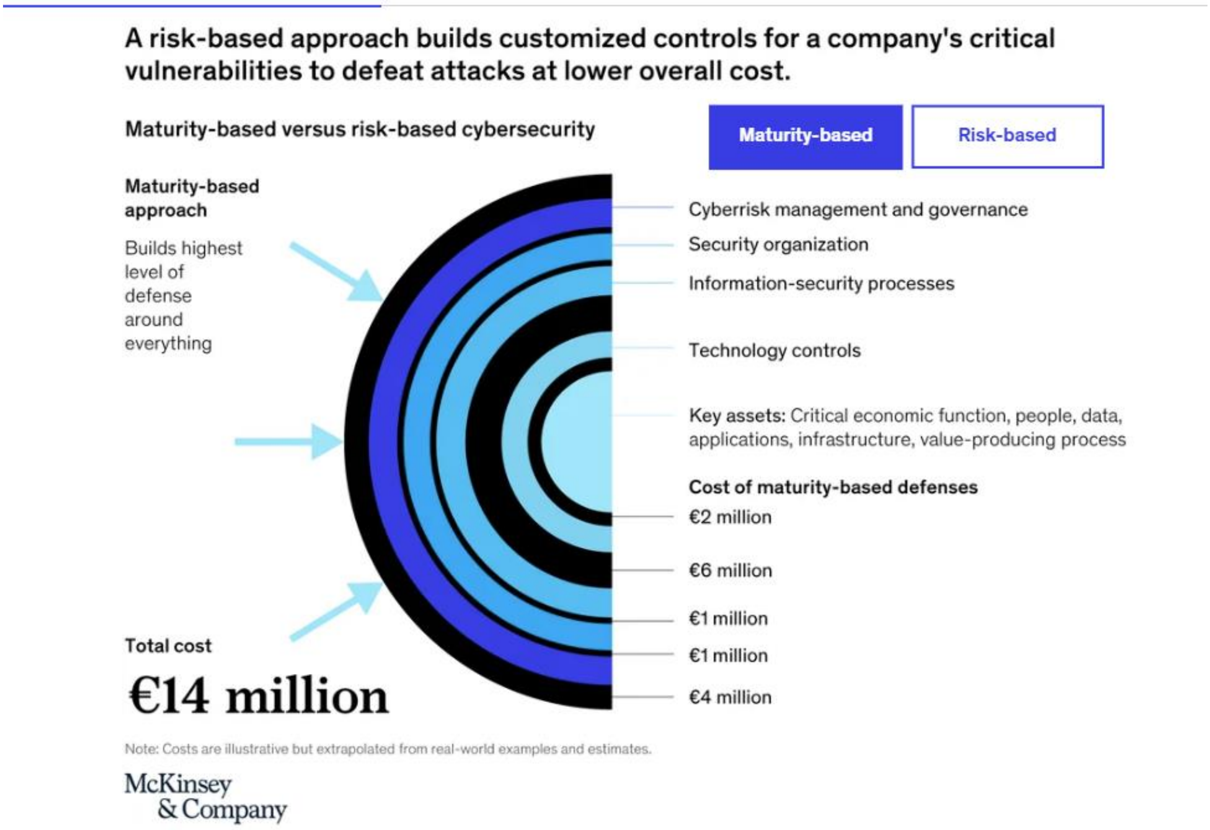
Example activities

- ○ Deploy advanced analytics and machine learning for preventative detection
- ○ Implement security by design with multilayer response-time reduction

Advanced

McKinsey & Company

Going by the earlier quote is this an option or a need for critical infrastructure companies is a part of regulatory decision. National Emergency Management Bill can consider that aspect for at least critical infrastructure and offer companies a plan of action or some time for them to adopt these ideas.



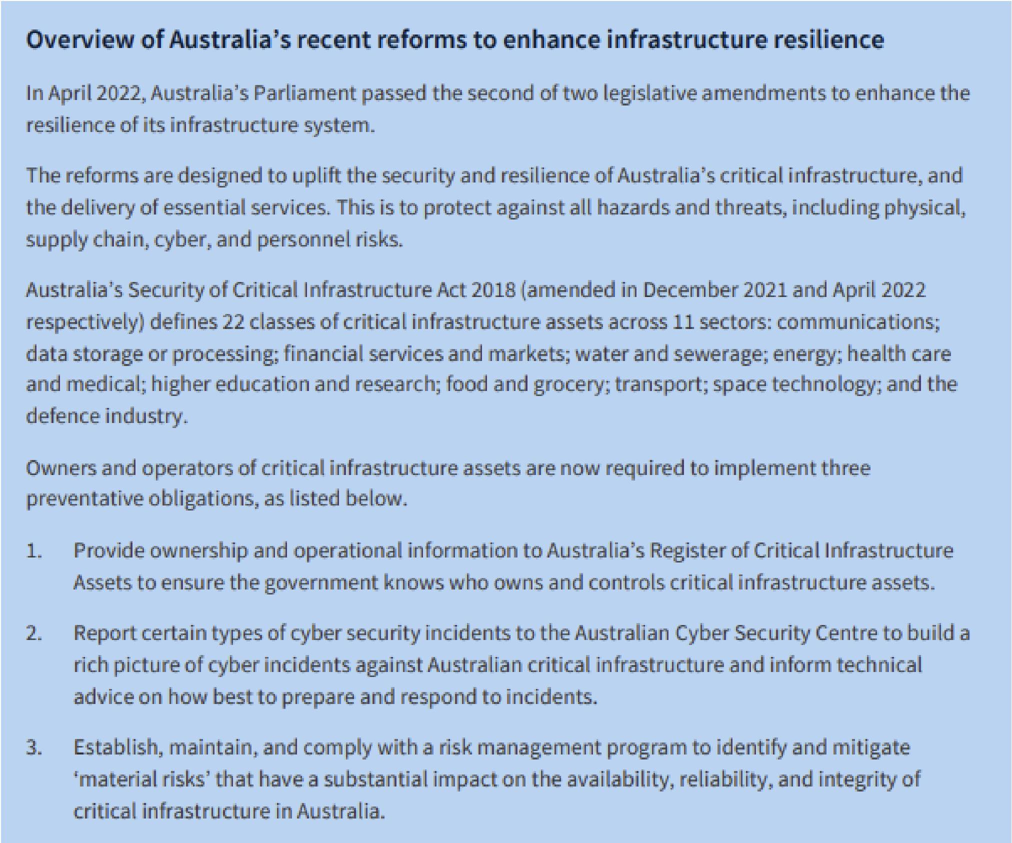
A risk-based approach builds customized controls for a company's critical vulnerabilities to defeat attacks at lower overall cost.

Maturity-based versus risk-based cybersecurity

Note: Costs are illustrative but extrapolated from real-world examples and estimates.

McKinsey & Company

This was envisaged by the discussion document too though the context is from a foreign country the concept remains the same. For more guidance to a risk based approach to cybersecurity the resource can be referred and contextualised The approach to risk-based cybersecurity | McKinsey.



Overview of Australia's recent reforms to enhance infrastructure resilience

In April 2022, Australia's Parliament passed the second of two legislative amendments to enhance the resilience of its infrastructure system.

The reforms are designed to uplift the security and resilience of Australia's critical infrastructure, and the delivery of essential services. This is to protect against all hazards and threats, including physical, supply chain, cyber, and personnel risks.

Australia's Security of Critical Infrastructure Act 2018 (amended in December 2021 and April 2022 respectively) defines 22 classes of critical infrastructure assets across 11 sectors: communications; data storage or processing; financial services and markets; water and sewerage; energy; health care and medical; higher education and research; food and grocery; transport; space technology; and the defence industry.

Owners and operators of critical infrastructure assets are now required to implement three preventative obligations, as listed below.

1. Provide ownership and operational information to Australia's Register of Critical Infrastructure Assets to ensure the government knows who owns and controls critical infrastructure assets.
2. Report certain types of cyber security incidents to the Australian Cyber Security Centre to build a rich picture of cyber incidents against Australian critical infrastructure and inform technical advice on how best to prepare and respond to incidents.
3. Establish, maintain, and comply with a risk management program to identify and mitigate 'material risks' that have a substantial impact on the availability, reliability, and integrity of critical infrastructure in Australia.

In the light of new attacks this is a need and more stringent regulation to increase accountability of companies foreign or Kiwi to be socially responsible such as filing information about cyber incidents. SEC notice to SolarWinds CISO and CFO roils cybersecurity industry - Reseller News (an example is key man accountability for more motivation to work harder for inbuilt resilience).

Document quote:
Critical infrastructures operate as a system. Each critical infrastructure depends on services provided by other critical infrastructures (e.g., many power grid functions rely on telecommunications). The breadth and depth of connections between infrastructures, means that vulnerabilities in any critical infrastructure asset can pose risks to the entire system's stability.

These features can make it more difficult to build appropriate levels of resilience without government intervention. This is because: a. the costs of infrastructure failure are spread widely across the community, but the costs of enhancing resilience are borne by individual infrastructure entities. Given that critical infrastructure owners and operators only have financial incentives to an amount equal to their own potential losses of infrastructure failure, this can create a gap between the level of resilience optimal for the infrastructure entity and the 'socially optimal' level of resilience.

Feedback: *So, this is a direct quote from the document so US/UK guidelines for inbuilt resilience in infrastructure, Industrial Control System security and OT system security is being re-emphasised, it is a ROI based approach than a cost.*

Standards can apply to a critical infrastructure entity (the approach taken under the CDEM Act 2002), or to its critical assets (the approach taken under Australia's Security of Critical Infrastructure Act). Linking standards to critical assets, rather than the entities that are responsible for them, may be a better way to target expenditure. This is particularly true for infrastructures that provide a range of critical services, only some of which are critical.
Feedback: This is good approach but who retains accountability for standardising critical assets? For instance, an electricity distributor or water pipeline distributor may be a company but who is the one being influenced if there is an outage? Accountability will reduce chance of attacks and increase efforts at resilience?

Critical infrastructure entities at the very core of the system generate large spill overs that have farreaching impacts. Implementing minimum standards would help reduce the risk of weaknesses in one entity adversely impacting the entire infrastructure system, but it would not eliminate the risk entirely. This is because minimum standards might not be stringent enough for critical infrastructures that are nationally important – for example, those that have a significant number of connections with other critical infrastructures and therefore crucial to the overall stability of the infrastructure system (e.g., some energy or telecommunications providers).

For this reason, some jurisdictions impose additional requirements on their most important critical infrastructures. This is similar to the concept of Globally and Domestically Systemically Important Banks, which must hold additional capital, relative to less important banks, to manage risks to the whole banking system.

This kind of proportionate and risk-based regulatory approach, where resilience requirements are tied to an infrastructure's importance, has many advantages.

These include:

prioritising spending on resilience investments that would have the most significant impact for New Zealand's infrastructure system.

reducing the risk that resilience requirements are set so high for all critical infrastructure entities that they create undue barriers to entry, reducing competition.

Feedback: Will stringent measures be useful for high risk and high impact areas? Colonial Pipeline attack is a great example in the US. My point is accountability with stringent guidelines and trust but verify approach from a cyber perspective.

Disparity in resilience requirements between infrastructure sectors can also undermine the value of investments that some critical infrastructure entities are already making to enhance their own resilience. For example, a high level of resilience in the financial sector may not effectively mitigate outages or disruptions to electronic payment systems, if the services that they rely upon (e.g., electricity and telecommunications) are not comparatively reliable.

Feedback: For a gamut of systems PCI Compliance and regulations may help Payments and Settlements Act. *Microsoft Word - A2007-51 _1_.docx (ifsca.gov.in)*

A few years back a SWIFT Banking fraud affected Bangladesh SWIFT banking system frauds shows that even trusted financial institutions are vulnerable to attack (theconversation.com).

Discussion document quotes:

Some clauses can be introduced in Emergency Management Bill. However, the Emergency Management Bill (and existing requirements for lifeline utilities) focuses on emergency management, rather than critical infrastructure resilience. While the Bill would reinforce the need for resilience, the government – would still be unable to:
a. applies more stringent mandatory requirements to more critical assets.
b. applies specific requirements to manage particular risks or vulnerabilities (e.g., minimum cyber security standards to protect networks from malicious cyber activity)
c. determines whether the Bill's requirements are being met or met in a consistent way (i.e., assess whether critical infrastructure entities are compliant)
d. takes enforcement action before or after an emergency event, if it is determined that resilience requirements were not met.

Feedback: Whichever ideas seem less of a regulatory burden can be considered for a proposed clause in the bill. Mature approach to resilience starts with baby steps.

Discussion document quotes:

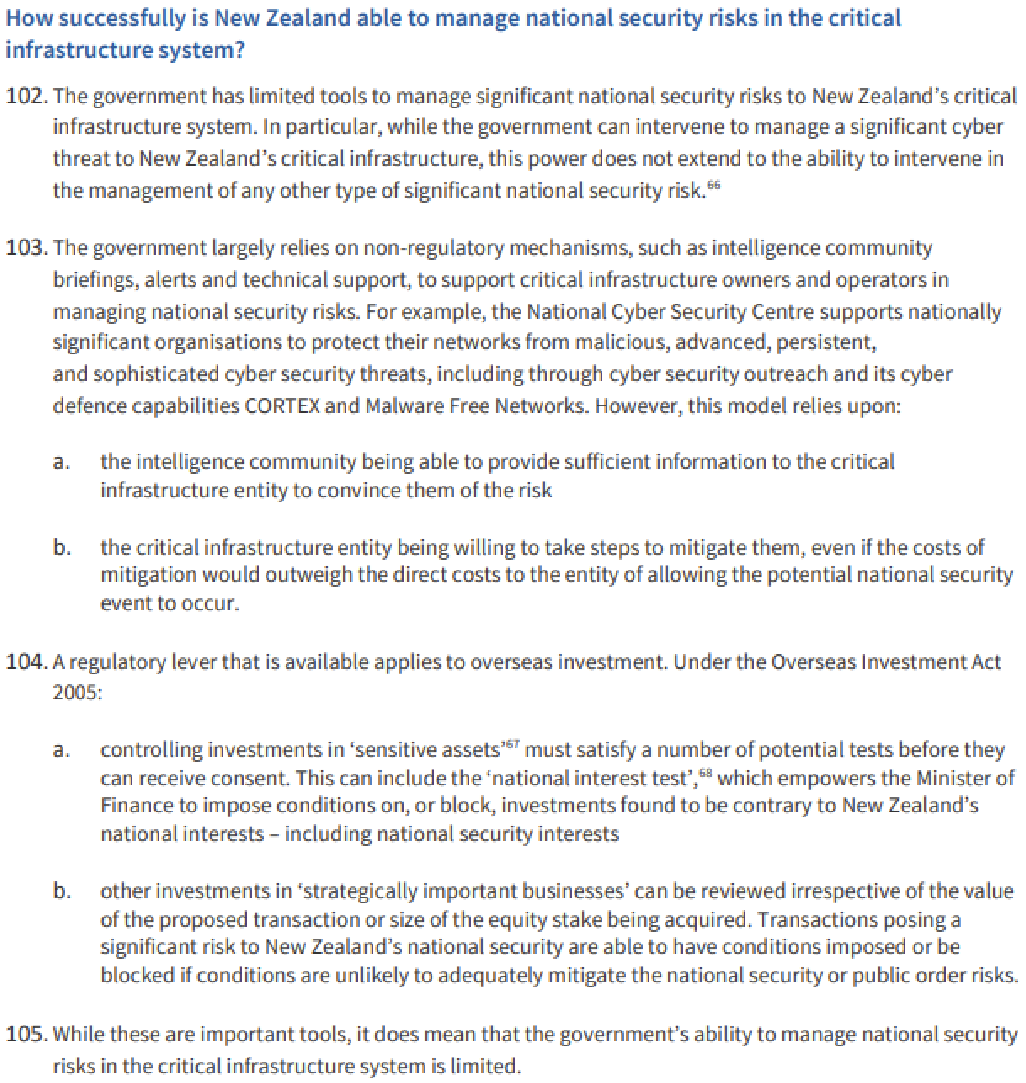
it may not always be possible to work collaboratively with a critical infrastructure owner or operator to manage a risk due to:

a reliance upon classified information that may not be possible to share.
disagreement between the government and the critical infrastructure entity over the risk, or the mitigations necessary to manage it.

a need to act immediately to protect New Zealand's national interests, where consultation or collaboration is not possible given the constraints.

the infrastructure owner or operator being unwilling to manage the risk.

Feedback: A lot of great points in the document but if we do not have a clause which enforces information sharing or overcomes barriers to infrastructure resilience will it be in the country's interest? ***Australia has a Minister involved but is that very high level, a Directorate potentially can be more far reaching for a unified approach to critical infrastructure resilience.***



How successfully is New Zealand able to manage national security risks in the critical infrastructure system?

102. The government has limited tools to manage significant national security risks to New Zealand's critical infrastructure system. In particular, while the government can intervene to manage a significant cyber threat to New Zealand's critical infrastructure, this power does not extend to the ability to intervene in the management of any other type of significant national security risk.[66]

103. The government largely relies on non-regulatory mechanisms, such as intelligence community briefings, alerts and technical support, to support critical infrastructure owners and operators in managing national security risks. For example, the National Cyber Security Centre supports nationally significant organisations to protect their networks from malicious, advanced, persistent, and sophisticated cyber security threats, including through cyber security outreach and its cyber defence capabilities CORTEX and Malware Free Networks. However, this model relies upon:

    a. the intelligence community being able to provide sufficient information to the critical infrastructure entity to convince them of the risk

    b. the critical infrastructure entity being willing to take steps to mitigate them, even if the costs of mitigation would outweigh the direct costs to the entity of allowing the potential national security event to occur.

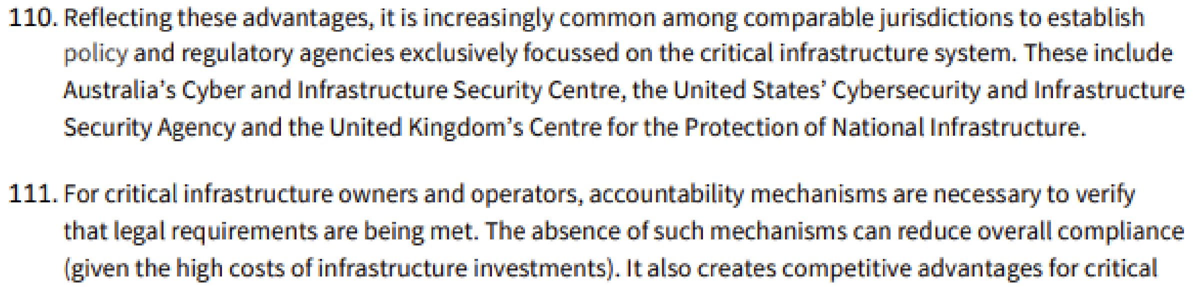
104. A regulatory lever that is available applies to overseas investment. Under the Overseas Investment Act 2005:

    a. controlling investments in 'sensitive assets'[67] must satisfy a number of potential tests before they can receive consent. This can include the 'national interest test',[68] which empowers the Minister of Finance to impose conditions on, or block, investments found to be contrary to New Zealand's national interests – including national security interests

    b. other investments in 'strategically important businesses' can be reviewed irrespective of the value of the proposed transaction or size of the equity stake being acquired. Transactions posing a significant risk to New Zealand's national security are able to have conditions imposed or be blocked if conditions are unlikely to adequately mitigate the national security or public order risks.

105. While these are important tools, it does mean that the government's ability to manage national security risks in the critical infrastructure system is limited.

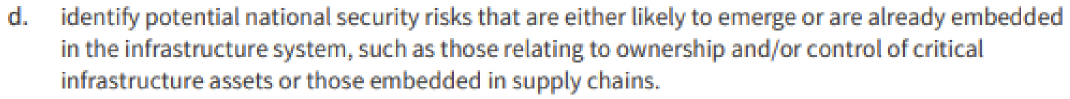
This is a direct quote from the discussion document if a Directorate with more judicial powers and an Act similar to Australia Critical Infrastructure Act is in place will it reduce issues? Ministers are too high to be able to deal with smaller areas. A team of skilled consultants with resilience experience for different areas would be a more pragmatic and effective solution (benefits outweigh costs if we do not resolve issues in hindsight). Accountabilities are with crown entities and private players as suggested earlier. If private companies are consulted, they will call it burdensome, but the customers or kiwis will not find it useless. If there is no electricity supply the company is impacted but so are people.



110. Reflecting these advantages, it is increasingly common among comparable jurisdictions to establish policy and regulatory agencies exclusively focussed on the critical infrastructure system. These include Australia's Cyber and Infrastructure Security Centre, the United States' Cybersecurity and Infrastructure Security Agency and the United Kingdom's Centre for the Protection of National Infrastructure.

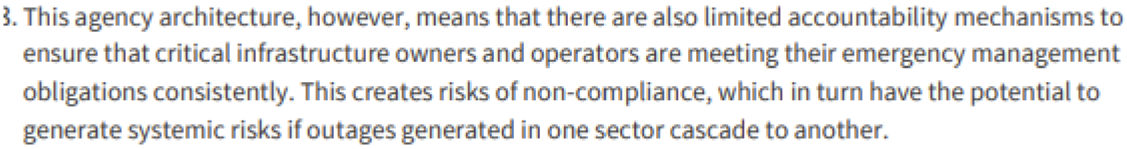
111. For critical infrastructure owners and operators, accountability mechanisms are necessary to verify that legal requirements are being met. The absence of such mechanisms can reduce overall compliance (given the high costs of infrastructure investments). It also creates competitive advantages for critical

Beautifully quoted by the discussion document and the international best practices are being referred in my humble submission. USA, UK etc.

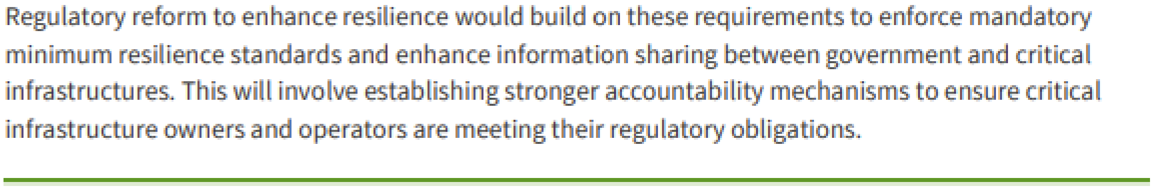


d. identify potential national security risks that are either likely to emerge or are already embedded in the infrastructure system, such as those relating to ownership and/or control of critical infrastructure assets or those embedded in supply chains.

If ownership and accountability are not with the company, is it not an undue advantage for the infrastructure operators?

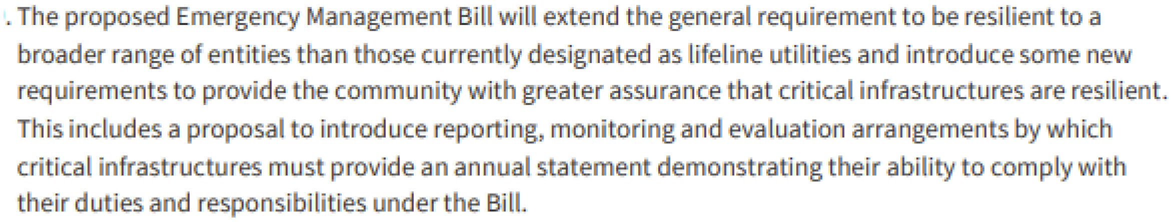


3. This agency architecture, however, means that there are also limited accountability mechanisms to ensure that critical infrastructure owners and operators are meeting their emergency management obligations consistently. This creates risks of non-compliance, which in turn have the potential to generate systemic risks if outages generated in one sector cascade to another.



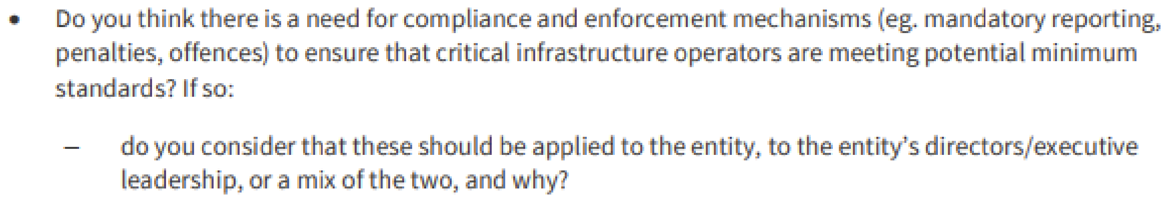
Regulatory reform to enhance resilience would build on these requirements to enforce mandatory minimum resilience standards and enhance information sharing between government and critical infrastructures. This will involve establishing stronger accountability mechanisms to ensure critical infrastructure owners and operators are meeting their regulatory obligations.

The document answers the question of accountability it creates a loophole with limited accountability. More than information sharing proactive risk detection or threat monitoring could be an emphasis for accountability perspective. Independent oversight of response mechanisms such as Financial Audit reduces risk of conflict of interest.



. The proposed Emergency Management Bill will extend the general requirement to be resilient to a broader range of entities than those currently designated as lifeline utilities and introduce some new requirements to provide the community with greater assurance that critical infrastructures are resilient. This includes a proposal to introduce reporting, monitoring and evaluation arrangements by which critical infrastructures must provide an annual statement demonstrating their ability to comply with their duties and responsibilities under the Bill.

Excellent point risk dashboards such as in Financial Audits and SEC/Regulatory oversight for cyber risks can be an effective manner to strengthen proactive risk-based resilience activities. USA does that and NZ can consider it in the future than in hindsight.



- Do you think there is a need for compliance and enforcement mechanisms (eg. mandatory reporting, penalties, offences) to ensure that critical infrastructure operators are meeting potential minimum standards? If so:
  - do you consider that these should be applied to the entity, to the entity's directors/executive leadership, or a mix of the two, and why?

The executive leadership and managers since it are a shared responsibility to monitor activities. Senior management is responsible for corporate/ government affairs. If not, a legal leeway for noncompliance or using weak system exists and so does risk of conflict of interest, so independent audits is important to ensure there is governance oversight.