Marty Rickard - *Web form submission*

Critical Infrastructure Resilience

What is your name?

Marty Rickard

What is your email address?

marty@rickard.co.nz

Are you responding as an individual or on behalf of an organisation?

Individual

Do you consent for your submission (including identifying information) to be published and shared in lines with terms for this public consultation?

Yes

Do you consent for your submission (including identifying information) to be published and shared in lines with terms for this public consultation? - Please note what should be withheld and for what reasons.

[Nil]

Does more need to be done to improve the resilience of New Zealand's critical infrastructure system?

Absolutely. NZ is lagging far behind our partner countries. I see this every day in my work environment.

Have you had direct experience of critical infrastructure failures, and if so, how has this affected you?

Yes. I have been deeply and actively involved in the cyber security programmes of NZ based electricity generators and foreign critical infrastructure operators. This includes cyber security design, installation, operation and incident response, at GRC, operational, technological and architectural levels.

How would you expect a resilient critical infrastructure system to perform during adverse events?

I don't believe it is possible to have a zero-risk, zero-outage environment, however we should target minimal disruption and perhaps define that. This would include requirements to report and share all incidents and near misses to enable better learning and improvement.

Would you be willing to pay higher prices for a more resilient and reliable critical infrastructure system?

Is there another option? Businesses can't be expected to fund multi-million dollar mandated improvements without some downstream effect unless central government provides finance at low cost.

The work programme's objective is to enhance the resilience of New Zealand's critical infrastructure system to all hazards and threats, with the intent of protecting New Zealand's wellbeing, and supporting sustainable and inclusive growth. Do you agree with these objectives? If not, what changes would you propose?

In general, yes, although it feels as if this is 5yrs too late, but also, better late than never.

Do you agreed with the proposed criteria for assessing reform options? If not, what changes you would propose?

In general, yes.

Do you think the megatrends outlined pose significant threats to infrastructure resilience?

Yes.

Are there additional megatrends that are also important that we haven't mentioned? If so, please provide details.

I would be inclined to separate Artificial Intelligence from the general tech trend as this poses a more complicated threat and change to operational scenarios than the rest of the tech industry.

Do you think we have described the financial implications of enhancing resilience accurately? If not, what have we missed?

Perhaps a little understated. I am not convinced people realise the costs to implement these programmes.

How important do you think it is for the resilience of New Zealand's infrastructure system to have a greater shared understanding of hazards and threats?

Critical. Having been involved as a member of the CSSIE representing an electricity generator, the information sharing, communication and collaboration was generally very good and needed to be expanded to wider industries.

I have also experienced the lack of such sharing in other CI sectors and can say that this is critical to have this shared understanding.

If you are a critical infrastructure owner or operator, what additional information do you think would best support you to improve your resilience?

* Open threat and (where appropriate) intelligence sharing
* Common secure communication channels
* Mandated reporting of incidents

The first two made a huge difference defending critical infrastructure from cyber attack. The last one was noticeably missing.

What do you think the government should do to enable greater information sharing with, and between, critical infrastructure owners and operators?

More critical infrastructure information exchanges that openly intercommunicate as needed.

Would you support the government having the ability to set, and enforce, minimum resilience standards across the entire infrastructure system?

Yes. Align minimum standards with those used by our intelligence and military partners such as NIST, AESCSF etc.

Would you support the government investing in a model to assess the significance of a critical infrastructure asset, and using that as the basis for imposing more stringent resilience requirements?

Yes. I would suggest we look to adopt an Australian standard as we see in so many of the AS/NZS standards - SOCI, AESCSF etc... Other countries have done the hard work, we do not need to start from the bottom.

What criteria would you use to determine a critical infrastructure asset's importance? Investing in a model to assess a critical infrastructure asset's criticality, and using that as the basis for imposing resilience requirements that are more stringent on particularly sensitive assets?

Again, we do not need to reinvent the wheel. The US and Australia have done this already, and for the US in particular, it's proven and working. Refer NIST CSF, NERC-CIP, or for Australia, AESCSF, SOCI etc. These other nations have identified these criteria. We are not that different.

Do you think there is a need for the government to have greater powers to provide direction or intervene in the management of significant national security threats against a critical infrastructure? - Is there a need for greater powers? If so, what type of powers should the government consider? What protections would you like to see around the use of such powers to ensure that they were only used as a last resort, where necessary?

Yes.
* Mandated minimum compliance levels
* Ability to intervene and where necessary, shut down operators until compliance is achieved
* Enforcement options not unlike those in the NZ Health & Safety at Work legislation.
* Make executives liable for compliance

Do you think there is a need for a government agency or agencies to have clear responsibility for the resilience of New Zealand's critical infrastructure system?

* A single Agency - minimise red-tape and costs
* It may be possible to implement this in an existing agency, however a clean start may provide better outcomes
* Refer to other countries and their implementation

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?

Yes. Varying levels to the entity, the directors and executive leadership - much the same as under the NZ H&S at Work act. The H&S approach has been proven to work over the last 3-4 decades.

What additional comments do you have?

I can only really comment from a cyber security perspective, however in my role as a cyber security advisor and consultant to some of the worlds largest companies, I do get to see how they are affected by and implement their responses to the changing legislature in their theatres of operation.

NZ is lagging behind and our security statistics have shown that we are a spring-board, or jump-off point for attacks against our partners. We need to do better.

NZ is also taking approaches and relationships with certain foreign powers that increase our risk to their influence, which in turn increases risk to our infrastructure - I have seen this activity first hand.

We need to make changes and improve in order to remain a country that is respected as a good place to live life. We risk becoming another failed state if we don't change.