Cisco Systems - Web form submission

Critical Infrastructure Resilience

What is your name?

Matt Carling

What is your email address?

mcarling@cisco.com

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

Cisco Systems

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?

Cisco welcomes the opportunity to provide a submission to New Zealand's Strengthening the resilience of Aotearoa New Zealand's Critical Infrastructure System Discussion Document. Although only one aspect of critical infrastructure resiliency, a cyber-enabled country is critical for a healthy, growing economy.

New Zealand is recognised as a leading digital nation, ranking 8th out of 146 countries globally in the Cisco Digital Readiness Index. However, in March 2023, Cisco commissioned research to gauge organisations' own assessment of their readiness to meet modern security challenges and the results of the research were clear: no matter what kind of business you operate and no matter where you are, security resilience is imperative in today's hybrid world. The findings are documented in the Cisco Cybersecurity Readiness Index: Resilience in a Hybrid World .

The independent double-blind survey asked 6,700 cybersecurity leaders across 27 markets to indicate which solutions they had deployed, and the stage of deployment, across five key pillars - identity, devices, network, application workloads and data. Companies were then classified in four stages of increasing readiness: Beginner, Formative, Progressive and Mature.

• Beginner (Overall score of less than 10): At initial stages of deployment of solutions
• Formative (Score of between 11 – 44): Have some level of deployment, but performing below average on cybersecurity readiness
• Progressive (Score of between 45 – 75): Considerable level of deployment and performing above average on cybersecurity readiness

• Mature (Score of 76 and higher): Have achieved advanced stages of deployment and are most ready to address security risks

Alongside the stark finding that only 14% of companies in New Zealand are at the Mature stage, more than two thirds (69%) of companies fall into the Beginner (13%) or Formative (56%) stages – meaning they are performing below average on cybersecurity readiness. Globally, 15% of companies are at a Mature stage – that is, they have a cybersecurity posture that is mature enough to defend against the threats of a hybrid world.

As the scope of assets and sectors considered as critical infrastructure expands in New Zealand as is being observed in many other digitised nations, the need to uplift cybersecurity readiness as an element of resiliency becomes more pressing.

https://www.cisco.com/c/m/en_us/about/corporate-social-responsibility/research-resources/digital-readiness-index.html#/country/NZL

https://www.cisco.com/c/m/en_us/products/security/cybersecurity-reports/cybersecurity-readiness-index.html

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

[Nil]

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

[Nil]

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

[Nil]

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?

One of the objectives for the works programme (6.b.) is to extend New Zealand's regulatory approach including the imposition of consistent standards. Rather than bespoke country specific standards, Cisco supports the continued joint work of Standards Australia and Standards New Zealand in recognising and endorsing applicable international standards. The adoption of ISO/IEC 27002:2022 as AS/NZS ISO/IEC 27002:2022 being one example. Aligning to international standards will provide access to a wider range of global solutions and also remove barriers for New Zealand organisations to access overseas markets in return.

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

[Nil]

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

As noted in the paper, some New Zealand critical infrastructure sectors carry significant technical debt through outdated or legacy systems which may be costly or difficult to update yet are a prime exposure point in the current security environment. The question then posed is how to protect assets that cannot protect themselves? This is compounded by the rapid uptake of new technologies. As highlighted earlier, New Zealand organisations are leaders in digital readiness but this not matched by a similar ranking in cybersecurity readiness. To address this, whether by regulation or voluntarily, organisations need to assess and address the cyber risks to their operations as a standard business process.

The discussion paper provides an overview of the recent Australian SOCI reforms. Of note in the implementation of the reforms are not only are impacted organisations afforded a gradual period of implementation, but SOCI recognises many Australian sectors (as is the case in New Zealand) already meet many obligations through existing regulators or industry norms. Recognising existing schemes then avoids additional financial costs and effort to some sectors. Additionally, SOCI recognises that critical infrastructure assets may be owned by organisations of very different size, hence flexibility is afforded on adopting risk assessment approaches or security frameworks that are suitable for each organisation - rather than mandating a single approach for all. For example, a smaller Australian organisation can demonstrate treating cybersecurity risks by following the ACSC Essential 8 maturity levels whereas a large organisation can adopt and certify to a more comprehensive (and expensive) ISO/IEC 27001 standard or similar. New Zealand should consider similar flexibility to limit the financial implications especially on smaller organisations.

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

[Nil]

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

[Nil]

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?

A shared understanding of hazards and threats between sectors is critical where there are cross-sector dependencies as identified in the discussion paper (70.e)

Using an example of a cloud service offering, the criticality of the cloud service in contributing to resilience is dependent on the business impact to the consumers of that cloud service. Potentially, risks could be treated within the delivery of the cloud service but equally it could be treated by the cloud consumer through diversity of supply, failover arrangements, or other business continuity plans.

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

[Nil]

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

Information sharing needs to be timely and actionable. For example, in the cybersecurity domain, the constantly reducing window between vulnerability discovery or announcement and malicious exploitation requires moving to "machine-speed" response. That includes machine-speed information sharing. Any initiatives towards delivering on this this goal would be beneficial.

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

The discussion paper provides an overview of the recent Australian SOCI amendments. Of note, the Australian obligations are principled based. The Risk Management Program obligation to treat the four identified hazards permits organisations to select standards or treatments that are appropriate to their sector, their organisational size, and their maturity. Whilst the New Zealand government could and should provide examples of minimum resilience standards, the government should avoid limiting organisational choice of a standard – but rather obligating the organisation to select and follow one which is appropriate.

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?

[Nil]

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?

There are some classes of assets where their criticality for essential services such as electricity generation and distribution or the provision of potable water can be more readily be identified by existing regulators and asset owners themselves. Complexity arises where the sector has one or a few dominant providers and many smaller providers or the sector is completely comprised of smaller providers. A threshold-based approach may be required to identify dominant players where a resilience impact would have a major sectorial impact versus a sector comprised of many smaller providers where resiliency is delivered by diversity of providers. As such, there is no single one size fits all approach – analysis and engagement with the expertise within each sector is required in developing criteria for critical infrastructure asset identification.
Some sectors such as the Data Storage and Processing Sector under the Australian SOCI Act are not critical in their own right but rather by the criticality of the workload or data they are hosting for an organisation in another sector. Only that other sector organisation has knowledge of criticality and a mechanism to formally advise (and discuss) with the provider is required.

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?

Mandatory directive and intervention powers raise many valid concerns for critical infrastructure operators both financially and reputationally noting also that in many sectors governments do not necessarily have the expertise of the sector itself when it comes to understanding the operational impact of changes or the technology itself. Any approval of mandatory directive powers needs to demonstrate the prior application of voluntary assistance, information sharing, and that a more collaborative approach has been refused or unsuccessful.

Additionally, whilst the use case for these directive and intervention powers is motivated by a national resiliency objective, that does not change the requirement of ICT providers and cloud service providers to operate (and be perceived to operate) independently of government interference globally. Hence, a mechanism should be included to review the application of any powers via a court or an independent authority to ensure appropriate oversight.

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?

There is at minimum a role for a co-ordinating function to avoid situations where an organisation may be subjected to multiple regulatory functions (or at least to the greatest extent possible). Issues arise where one sector provides critical services across multiple other sectors and is subject to the requirements of each other sector. Without co-ordination, lack of alignment between sectors in what is appropriate risk treat treatment of various hazards results in compliance complexity.

Any regulatory or compliance function whether linked to penalties or not should be appropriately isolated from the assistance and advice role of the New Zealand National Cyber Security Centre (NCSC). Cisco recommends this is formalised in a safe harbour agreement such that organisations can confidently engage the NCSC for assistance in a cyber incident without fear of regulatory repercussions. Organisations will still be subject to their regulatory obligations but in parallel to any immediate assistance needs.

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?

Cisco supports board and director accountability for addressing cyber security risk as one element of critical infrastructure resiliency, however this cannot be done in isolation of a complementary approach to board and director level education and awareness of these risks.

What additional comments do you have?

[Nil]