CREST International - *Web form submission*

Critical Infrastructure Resilience

What is your name?

Nigel Phair

What is your email address?

nigel.phair@crest-approved.org

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

Organisation

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?

We believe secure only makes a statement about a nation, an organisation or a system as a snapshot of a point in time. The New Zealand governments focus on resilience is correct as it encompasses becoming more secure but also recognises that it is important to be in a better position to deal with and withstand cyber attacks when they happen. Because they will happen. Cybercrime continues to evolve and as such the government's approach will need to be adaptive.
To achieve a more resilient cyber eco-system, it is essential to focus on building greater awareness of different tools, techniques and services that a public or private sector organisation need to use to protect itself and others.

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

CREST is an international not-for-profit, membership body representing the global cyber security industry. Our goal is to help secure a digital world for all by quality assuring our members and delivering professional certifications to the cyber security industry. We accredit over 300 member companies (with three members operating in New Zealand) across dozens of countries and certify thousands of professionals worldwide. Our members have regular, direct experience in responding to cyber security incidents surrounding critical infrastructure.

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?

We agree with the objectives of providing the government and citizens of New Zealand with assurance that any cyber attack on critical infrastructure assets will be dealt with professionally, competently and in a timely manner. To gain this assurance, the New Zealand government should ensure that owners and operators of critical infrastructure utilise cyber security professionals who can demonstrate their organisational and technical ability to do so.

To aid this assurance, CREST provides a suite of membership categories and personal certifications. Our members undergo a rigorous quality assurance process and employ competent professionals. Organisations buying their cyber security services from our members do so with confidence.

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

We think the government needs to consider all options which enhances resilience across all critical infrastructure sectors. Organisations that form part of New Zealand's financial services sector must remain resilient to cyber attacks. To help organisations achieve this goal, the Reserve Bank of New Zealand should implement the CBEST security assessment framework, as conducted by the Bank of England for their market. This is a similar approach to Australia's CORIE framework.

CBEST is tailored for the banking & finance sector, and is an intelligence-led penetration testing approach that mimics the actions of cyber attackers' intent on compromising an organisation's important business services and disrupting the technology assets, people and processes supporting those services.

CBEST differs from other security testing currently undertaken by the financial services sector because it is threat intelligence based, is less constrained and focuses on the more sophisticated and persistent attacks against critical systems and essential services.

CREST helped to develop the accreditation standards for CBEST penetration testing, based on the already stringent standards for assessing the capabilities, policies and procedures that CREST member companies have to achieve. CREST stands ready to help New Zealand obtain the same level of assurance in the financial services sector.

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

[Nil]

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

With respect to cyber security, we believe this is a critical component. The collection and dissemination of cyber threat intelligence will allow the owners and operators of critical infrastructure to make informed risk-based decisions to make their assets and organisations more resilient to a cyber attack.

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?

Private and public partnership is essential. Genuine collaboration between the government and industry is the only way to ensure a strong defence against cyber attacks. Along with its traditional sources of threat intelligence, government need to establish a cross government / industry sharing partnership. This will provide a platform for the government and the private sector to share threat intelligence quickly and confidentially.

Good threat intelligence is of course essential. And this needs to be a collaborative and bi-directional effort between government and industry. The government needs to provide a baseline intelligence for red teaming engagements, for example, with threat intelligence providers adding more specific industry intelligence. But it is important that both government and industry have assurance in the threat intelligence providers and the skills of analysts.

CREST offers a recognised career pathway – based on a suite of certifications – for those individuals within the threat intelligence arena. Additionally, CREST has a number of member companies accredited to deliver threat intelligence, the services of which can be located via the CREST 'buyers portal' on the CREST website. Additionally, CREST has a Focus Group dedicated to threat intelligence which has created guidance to help businesses find the right Cyber Threat Intelligence partner to better meet their security challenges. The report can be found at [http://www.crest-approved.org/wp-content/uploads/2022/04/CTI-in-Business-Context_2021.pdf].

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

Yes, we believe the government should play an active role in creating, implementing and auditing minimum resilience standards. Such minimum standards, particularly for the financial services sector should be based on the United Kingdom CBEST and the Australian CORIE framework of threat intelligence-led penetration testing.

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?

The New Zealand government should choose a model for ensuring greater resilience of the financial services sector against a cyber attack. The government should be based on the United Kingdom CBEST and the Australian CORIE framework of threat intelligence-led penetration testing. Similar schemes have been formed by overseas jurisdictions and continue to assess maturity against cyber-attack trends rising in frequency and sophistication.

CREST stands ready to assist the government to implement such a scheme (as it does in the United Kingdom).

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?

[Nil]

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?

Cyber criminals are increasingly targeting New Zealand's critical infrastructure. There are many factors that have led to this but the growing digitisation of industry and people's reliance on mobile technologies is significant. When it comes to legislation, it is important to look at existing cybercrime laws and make sure there are defined laws pertaining to all cybercrimes.

As technology evolves and attacks increase it is essential that the regulatory framework does too. Regulation is important and experience tells us that while something is not mandatory, compliance will be low. Having a regulatory framework for an industry is also complicated by the increasingly complex and global digital supply chains most industries operate in. This is where taking advantage of global standards is important. It is important also to both consider improving supply chain resilience when considering any new regulation, but also doing that without making it prohibitively difficult to conduct business.

But Government cannot do this without the help and the support of industry collaboration to get it right. It also must consider global standards. Professional bodies like CREST also have an important part to play, working with its industry members to establish frameworks that do exactly what they need to do. And also, to monitor and report on compliance.

At CREST, we have worked with governments globally to establish and administer frameworks for several critical industries. There is no one size fits all solution. The level of regulation depends on the industry, whether it is part of critical national infrastructure and also the consequences of a cyber attack. And while regulatory frameworks will have many parts that are consistent across industries, it is important to ensure they are right for the specific market needs and the threats that sector faces.

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?

[Nil]

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?

[Nil]

What additional comments do you have?

CREST is an international not-for-profit, membership body representing the global cyber security industry, stands ready to help the New Zealand government improve the cyber resilience of the critical infrastructure sector. Our goal is to help secure a digital world for all by quality assuring our members and delivering professional certifications to the cyber security industry. We accredit 300 member companies across dozens of countries and certify thousands of professionals worldwide (including New Zealand). We work with governments, regulators, academe, training partners, professional bodies and other stakeholders around the world.

Our members undergo a rigorous quality assurance process and employ competent professionals. Organisations buying their cyber security services from our members do so with confidence.

To achieve a more resilient cyber eco-system, it is essential to focus on building greater awareness of different tools, techniques and services that a public or private sector organisation need to use to protect itself and others.

In the cyber security market, there is all too often misalignment of expectations and outcomes, when procuring services from a market that has very little governance, oversight or regulation. For example, while buyers recognise that cyber security involves technical assurance, they may believe that vulnerability assessment, penetration testing and red teaming all mean the same thing. This results in some buyers procuring one type of service and receiving something different that doesn't meet their needs. This problem exists across the fields of penetration testing, incident response, threat Intelligence and (SOC) Security Operations Centres.

This issue is compounded by the difficulty selecting the best service provider. Organisations, both public and private, need assurance that they can trust them to do what is needed, to do it properly and ethically.
Standards that define the service itself and also provide assurance in the supplier would help all organisations in Australia to easily identify who is the right supplier for their specific (and their

industry's) requirements and one that will improve their resilience. This is paramount to a more resilient nation.

CREST has created a range of research reports and best-practice guidance which inform both governments and industry on the benefits of a close working relationship to solve cyber security challenges. CREST has a range of membership options, certification pathways and professional development opportunities, all designed to raise the standards in the global cyber security industry. CREST has had an Australasian Chapter since 2012 and stands ready to work closely with all tiers of government to create more qualified and competent cyber security professionals.

We recommend the New Zealand government mandate all owners and operators of critical infrastructure to use CREST accredited individuals working for CREST approved companies to solve their cyber security challenges. CREST's online buyer search facility provides easy access to information on which companies to choose, even where buyers are not sure what services they need.

More information on CREST can be found at: [https://www.crest-approved.org/].