ENHANCING THE RESILIENCE OF OUR CRITICAL INFRASTRUCTURE

BY **GUY FINNY,** ASSOCIATE DIRECTOR – INFRASTRUCTURE & CAPITAL PROJECTS; AND **JOHN MARKER**, PARTNER – NATIONAL INFRASTRUCTURE LEADER, DELOITTE

Our society is reliant on the uninterrupted delivery of critical infrastructure services in an operating environment that has become increasingly complex and hazardous. Examples of compromised critical infrastructure have dominated recent headlines. Illustrative of this, Australian telecommunications provider Optus suffered a major data breach resulting from a cyber attack. On the other side of the world, critical European gas infrastructure has also suffered significant damage in apparent acts of sabotage.

The increasingly complex and hazardous world these organisations have had to navigate since the start of COVID-19 is now being recognised as part of a progression to a new normal. In response, regulators, boards and management are evolving practices, including application of an 'all hazards' approach to security and resilience. Australia has recently leveraged the all-hazards concept in codifying new risk management measures as part of a nation-building exercise to improve the overall resilience of the country's critical infrastructure.

New Zealand is not immune to these global trends. Critical infrastructure providers here should be turning their eyes to the horizon and ensuring that they are aligned with global best practice.

AN ESCALATING THREAT ENVIRONMENT

Critical infrastructure provides the essential services that underpin our society and economy. That includes infrastructure supporting energy, transport, communications, health, financial, data storage, education, defence, food supply and water services.

Critical infrastructure organisations are expected to deliver their essential services no matter what challenges they face. Rapidly changing domestic and global factors are seriously testing business practices as the world migrates to a more complex, post-pandemic operating environment. In recent years, critical infrastructure organisations have had to contend with cyber attacks, supply chain disruption, a pandemic and increasing geopolitical tensions. Climate change is also factoring more frequently and acutely into the creation of many highly disruptive physical and human hazards.

On top of this is the fact that critical infrastructure organisations are themselves becoming increasingly complex and interdependent. Physical assets increasingly have digital interfaces, and the delivery and maintenance of these assets is reliant on multilayered global supply chains.

Guy Finny

John Marker

BEST PRACTICE IS EVOLVING TO REFLECT THE NEW NORMAL

The ability to anticipate, prepare and adaptively respond to disruption and change is crucial to the continued effectiveness of our critical infrastructure. In the current environment, governments, boards and management are all increasingly aware of the need to evolve practices to ensure that they are still fit for purpose. A service failure can have significant adverse economic, commercial and reputational impacts – exposing firms to potential litigation risk if they fail to take reasonable steps to understand and mitigate hazards that are becoming more foreseeable.

Given the stakes, governments are also taking steps to enhance capabilities and embed resilience requirements into legislation.

The policy rationale for intervention is driven by the fact that interference or damage to critical infrastructure assets

can cause widespread disruption throughout society. While the failure of an asset can be extremely damaging to the reputation and financial viability of its owner, the costs to society of an entity failing to mitigate hazards to a critical infrastructure asset can be orders of magnitude larger than the losses accruing to that entity. To address this potential mismatch in incentives, governments are establishing critical infrastructure programmes and agencies, such as the United Kingdom's Centre for the Protection of National Infrastructure, and the Cybersecurity and Infrastructure Security Agency in the United States, with the objectives of introducing and enforcing requirements to improve the maturity of critical infrastructure entities in identifying and responding to risk.

In Australia, changes to the *Security of Critical Infrastructure Act 2018* have created an obligation for responsible entities to create and maintain a critical infrastructure risk management program. When these changes come into force, relevant entities will be required to identify and, as far as is reasonably practicable, take steps to minimise or eliminate material risks on an all-hazards basis. Boards will have to attest to the risk management program, and while there are penalties for noncompliance, it is the implications for fiduciary duties that is really driving directors to take notice and support change.

THE ALL-HAZARDS LENS

A key departure for the Australian legislation is the requirement to consider risk more holistically by applying an all-hazards lens at an asset level. This is a significant change from traditional risk management approaches that apply a more enterprise-level lens. An asset level focus requires organisations to understand, identify and manage hazards to their critical assets – including physical and natural hazards, supply chain hazards, personnel hazards, and cyber and information hazards – that, at the end of the day, have the greatest potential to impact delivery of their essential services.

This approach not only deepens the organisation's risk knowledge base, it also helps break down siloes between different functions – revealing a true picture of the organisation's resilience maturity.

Deloitte's Critical Infrastructure practice has been active on both sides of the Tasman, helping critical infrastructure entities deploy this approach to uplifting resilience.

CHANGE IS ON THE WAY FOR NEW ZEALAND

The government, through its response to the infrastructure strategy, has stated that it supports, in full, the New Zealand Infrastructure Commission's proposal to increase the resilience of critical infrastructure. New Zealand's regulatory framework for critical infrastructure is currently contained in the *Civil Defence Emergency Management Act 2002*, which outlines requirements for identified 'lifeline utilities' to ensure that they can function during and after an emergency.

In the short term, proposed changes to the Civil Defence Emergency Management Act will see the concept of 'critical infrastructure' explicitly embedded in legalisation.

The infrastructure sector should be paying particular attention to potential changes anticipated to occur over the medium term – the government has tasked officials with considering whether more fundamental changes are required to guarantee critical infrastructure resilience. Based on international examples, it is likely that we will see change through a work program that will weigh up the benefits and costs of the following potential reforms:

- establishment of a critical infrastructure centre of excellence in government to develop guidance and best practice for New Zealand's critical infrastructure
- introduction of requirements for specific critical infrastructure entities to prepare and implement risk management plans be prepared on an all-hazards basis
- introduction of enhanced information-sharing obligations with government
- introduction of enhanced governance obligations, including requirements for board attestation regarding critical infrastructure resilience.

The government expects to begin consultation with the sector in the first half of 2023.

GETTING AHEAD OF THE CURVE

Ahead of this consultation, critical infrastructure entities should build a deep understanding of their organisation's approach to resilience and its effectiveness in the current landscape. This will not only help organisations better align themselves with international best practice, it will also enable them to articulate and constructively engage with policymakers through the regulatory reforms on the horizon for our critical infrastructure. //