POCKET REVIEW

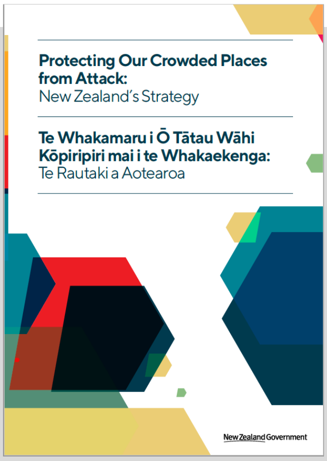
29/04/2021

PROTECTING OUR CROWDED PLACES FROM ATTACK: NEW ZEALAND'S STRATEGY

NZ Government (hosted on NZ Police site)

Published August 2020 (20 pages).

https://www.police.govt.nz/sites/default/files/publications/crowdedplaces-strategy-30092020.pdf



Protecting Our Crowded Places from Attack:
New Zealand's Strategy

Te Whakamaru i Ō Tātau Wāhi Kōpiripiri mai i te Whakaekenga:
Te Rautaki a Aotearoa

New Zealand Government

> *"... trusted relationships .. and a way to translate threat information into effective, proportionate protective security measures."*

WHAT IS IT?

A strategy to help owners and operators of crowded places protect the lives of people working in, using and visiting their crowded place, from the risk of organised or terrorist attack.

Outlines the government agency responsibilities, and gives guidance to owners and operators of crowded places.

The document is designed to be read alongside the 'Crowded places resources' - self-assessment, tools and posters (refer link below).

WHY READ IT?

Provides a good overview of roles and responsibilities and a summary of how government agencies assess risk.

Although written in the context of terrorism preparedness, the standard tools for site assessment, and the risk management process, also link well with general site security - e.g. robbery/burglary and workplace violence.

Read alongside:

- Australian Strategy for Protecting Crowded Places from Terrorism
- NZ Police Crowded Places resources

This document is an unsolicited, independent summary of a public domain reference.

Key messages for owners and operators

The strategy is based on four elements: Building stronger partnerships, Enabling better sharing of information and guidance, Implementing effective protective security, Increasing resilience.

The Government works with NZ and Australian agencies to monitor threats and produce guidelines.

Police and local government are key partners for interagency advisory group information, recommending owners/operators seek further professional advice, and to ensure compliance (including the responsibility of owners & operators of to assess risks of attack and implement, monitor & review mitigations.

Owners and operators should consider 'layered security':

- Deter - Through obvious physical and electronic target hardening
- Detect - Visual detection and alert systems.
- Delay - Physical counter measures and processes
- Respond - Timely and coordinated reaction by security staff.

Monitor the current national terrorism threat level and implications for the business operations.and contingency measures.

In the event of an attack (posters available): Escape, Hide, Tell.

Considerations:

- Resilience is a corporate responsibility, makes good business sense, supports the business reputation and may save lives & minimise harm.
- Keep mitigations in proportion to risks
- Monitor the effectiveness of mitigations
- Review mitigations at appropriate times

In the event of an attack

ESCAPE
Move quickly and quietly away from danger, but only if it is safe to do so

HIDE
Stay out of sight and silence your mobile phone

TELL
Call the Police by dialling 111 when it is safe

www.police.govt.nz/crowdedplaces

New Zealand Government

English

'In the event of an attack' poster - from Police website.

CONTENTS - NOTES

Attackers may focus on crowded places for several reasons:

- Mass casualty potential, psychological impact, easy to access, symbolic value, disrupt surrounding businesses & infrastructure, more witnesses, coverage and attention.

People preparing/underaking an attack display certain behaviours:

- Skills, knowledge, opportunities, motivation, group makeup and objectives influence attack size, style, sophistication, location & likelihood of success.

Attack resilience planning

Consider:

- The purpose of the place (e.g. presence of high-profile individuals), history of incidents, presence of high-risk facilities nearby, existing security, prevailing advice, mitigations for clear line of observation.

Owners, personnel (including private security personnel with direct responsibility) and bystanders may be able to detect suspicious behaviour.

Building an effective security culture is central to increasing resilience.

- Executive endorsement, commitment, compliance, risk assessment, staff buy-in, internal/external comms, screening, training & exercises, review, reporting and staff encouragement & reward.

Resilience to attacks should be a part of the Business Continuity Plan.

- Government would support affected owners and operators in an event.
- A robust BCP will often include; Cross training staff/volunteers, documented procedures, relocation sites, remote access, alternative equipment sources, secure offsite data, out-of-hours contact arrangements.
- Police or a coroner may need to override some elements in a BCP.

REVIEW AND COMMENTS

As a strategic-level resource, the document gives high-level guidelines.

There is an assumption that owners and operators of places with a higher risk profile (or needing more support) should seek specific guidance from:

- The named national groups established by the Police (CPAGNZ, BAGNZ, CAGNZ), and/or event-specific planning groups,
- Local government, and/or
- Private security specialists.

Although it is *not* specifically mentioned in the document, consider:

- Whether active planning may draw the **attention** of attackers.
- The need to keep planning records **secure**, e.g. physical/organisational vulnerabilities, hidden cameras, critical sites, codes or contingencies.
- The risk of **reputational** damage if planning is not transparent - e.g. accusations of profiling, discrimination, bias, or lack of trust in workers.
- **Ethics** and legality of technology - cameras, facial recognition, biometrics - especially where these may also be used to monitor staff.
- The need to define an **acceptable** level of attack risk, and to manage the risk perception of staff (or public) who may be concerned.

Take into account the **sensitivity** of planning, training and exercising a terrorist or coordinated attack. *If* the business has expert support and executive endorsement, it could be valuable to take a 'red team' approach, e.g. physical penetration testing (/plan) or simulating active surveillance.

It is important to note that the NZ "run(/escape), hide, tell" **approach** is the one also adopted in the UK and Australa. It is distinct from the "run, hide, fight" message a planner may encounter when reading US resources.