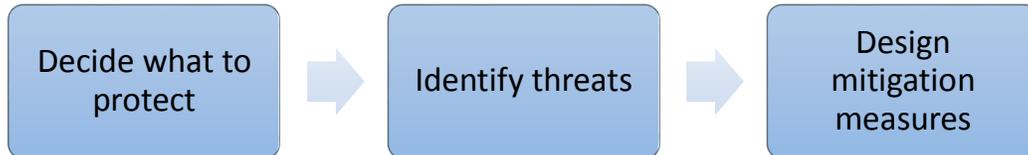# PROTECTIVE SECURITY ADVISORY FOR PREMISES

Premise owners should implement protective security measures to mitigate the risks of possible terrorist attacks.

HOW TO IMPLEMENT PROTECTIVE SECURITY MEASURES

Decide what to protect	→	Identify threats	→	Design mitigation measures

1.   DECIDE WHAT TO PROTECT

- Human lives are the topmost priority. You should thus know where employees and other premise users congregate.

- Identify other assets that are essential to your functions
  - E.g. Uninterrupted Power Supply (UPS) Room, Main or Intermediate Distribution Frame (MDF or IDF) Room, Sensitive Materials
  - Prioritise these assets based on how critical they are, to help you determine what measures to take to protect them.

2.   IDENTIFY THREATS

- Know the various forms that terror attacks can take:
  - Armed attackers – with firearms, knives or other weapons
  - Vehicles used as weapons
  - Explosives in a vehicle, on a person or in a bag or other containers
  - Chemical or biological agents

- Identify features of your premises that may increase the risk of an attack, or make you vulnerable to specific forms of attack.
  - Some examples: Areas of mass congregation in your premises that makes it an attractive target; close proximity of your premises to the road, which allow vehicles to be used as an effective weapon

3.   DESIGN MITIGATION MEASURES

- Review existing security measures to determine their effectiveness and identify gaps.

- o Things to consider include: CCTV systems, current model of deploying security staff, currency of standard operating procedures and emergency response plans.

- Based on your assets, threats and existing security measures, prioritise mitigation measures where risk is high. Consider the following:
    - o <u>Threat:</u> what is easiest for someone to attack?
    - o <u>Vulnerability:</u> which area in your premises is an attack most likely to succeed?
    - o <u>Consequence:</u> what areas will cause the greatest impact on your business if disrupted by an attack?

- Apply the 4Ds to mitigate risks according to your priorities – **Deter, Detect, Delay and Deny.**
    - o Measures to achieve the 4Ds come in the form of operations, technology and physical measures.
    - o

DETER – Prevent an attack by making it clear to an attacker that failure is likely. This includes having visible physical measures, presence of security officers and prominent signage that the premises are protected.

DETECT – Have ways to identify threats early and raise an alert. This includes looking out for potential attackers conducting reconnaissance or suspicious persons loitering. Threats can be detected by measures such as CCTV systems, intrusion detection systems, and bag and person checks.

DELAY – Create obstacles that can slow attackers down to allow more time to carry out contingency plans. Examples include forced-entry resistant doors, doors with electro-magnetic locks, physical barriers, or bollards to delay vehicles.

DENY – Ensure that only authorised persons can access important areas such, as the Fire Command Centre, Air Handling Units, safe rooms for hiding from an attacker, and other areas containing critical assets. Access control measures include biometric or card access, lock and key, and security clearance policies that allow you to differentiate staff and visitors.

For more information on developing contingency response plans, see our 'Contingency Planning Advisory for Premises'. EXAMPLES OF MEASURES TO REDUCE SECURITY RISKS

Operations Measures

- Limit access to floor plans and documents containing sensitive security information.
- Implement security checks at entry points, to deter and detect potential attackers and their weapons.
- Develop and exercise a building lock-down protocol
- Strict access control measures into protected areas, such as staff passes with biometric features, visitor escort, and card access
- Prepare the security team through relevant courses (e.g. Workforce Skills Qualifications Courses) and ensure that they are licensed to conduct checks on persons, vehicles and belongings
- Ensure security officers and staff are trained to recognise suspicious behaviour/items and to report them
- Have in place clear incident reporting procedures

Technology Measures

- Have adequate CCTV coverage of the building in line with the Video Surveillance Systems (VSS) standards, supplement CCTV with data analytic features where possible. The VSS standards can be found on the Police website at the following URL: http://police.gov.sg/img/advisories/misc/vss_standard_for_buildings.pdf
- Ensure security systems are maintained and operating effectively
- Install alarm systems
- Where feasible, consider having the capability to centrally lock down the different areas of the premises from the Fire Command Centre (FCC), so as to delay the advance of the perpetrator(s).

Physical Measures

- Adopt visible security measures, such as regular patrols by security officers around the perimeter of the building, and putting in place warning signs
- Have a clear line of demarcation between vehicular and pedestrian access so as to prevent vehicle ramming attacks into areas of mass congregation This may include the installation of bollards and planters to slow down a hostile vehicle should it attempt to attack pedestrians
- Have pre-identified rooms, preferably hardened, where employees can hide during an attack should evacuation become impossible.