4 Crowd Risks and Advanced Tools

The objectives of organisations engaged with crowd situations are subject to serious threats that can disrupt and compromise their integrity and prevent desired outcomes. By employing a risk management process, organisations can identify and assess threats, vulnerabilities and weaknesses and also the likelihood and consequences to the security environment.

Risk management involves identifying and assessing threats to the operating environment or strategic goals and prioritizing resources to minimise, monitor and control the impact of events (incidents). There are three key areas for assessing security related risks:

1. Information asset assessment
2. Threat assessment
3. Vulnerability assessment

Information assessment includes identifying physical and intangible assets and assessing the value of maintaining the ongoing cost or damages arising from loss. *Hazard/threat assessment* includes identifying potential threats, targets and the likelihood of occurrence. Potential threats include fraud, theft, loss of infrastructure and malicious acts. In assessing *vulnerability*, organisations need to understand the potential inadequacies and weaknesses. Threats differ across organisations and frequently change.

In an organisation affected by or controlling a crowd situation, risk management relates to a specific culture of processes that are engineered towards maximizing the objectives of the organisation. In managing the risks the organisation should take into account the function and objectives, as well as everyday operations. Organisation should seek to implement a positive risk culture and embed risk management practices into the day-to-day activities.

In developing a risk management process for crowd response and management, organisations should identify the following areas:

- Risks to people, information and assets and consequential impact on objectives, capability and preferred outcomes.
- The acceptable level of risk.
- Appropriate protections to reduce or remove risks.
- Assumptions – threats (arising from the intentions and capabilities when acted on), vulnerabilities, consequences, likelihood of occurrence.
- Responses and strategies of managing risk.

By adopting a risk-based approach to managing crowd-related risk, organisations can assess and prioritize activities and allocate resources to suit their requirements. Organisations should seek to implement multi-layered business architecture across the platforms to mitigate crowd related risks.

Organisations can be subject to serious threats that can disrupt and compromise their integrity. By employing a risk management process, organisations can identify and assess threats, vulnerabilities and weaknesses and the likelihood and consequences to the security environment.

The three important publications are:

1. International Electrotechnical Commission, International Standard, ISO/ IEC 31010:2009, First Edition, 2009.
2. Standards Australia/Standards New Zealand Standard Committee, AS/NZS ISO 31000:2009,Risk Management-Principles and Guidelines, November 2009.
3. International Organisation for Standardisation, ISO Guide 73:2009, Risk Management-Vocabulary, First Edition, 2009.

Definition(s) for the security of crowds

Protective security

- The framework implemented to identify, respond to and reduce the risk of harm from malicious acts.
- The measures to reduce the risk posed by malicious actors.

- Processes and activities that protect people, assets and information from malicious acts.

Physical security

Physical security is an essential part of protective security. It is approached from a risk-assessment basis and covers a wide array of assets and elements that require an increased level of protection from physical circumstances that may cause harm. Physical security extends to the protection of personnel, the layout and design of locations and institutions, as well as access to equipment, data, systems and networks.

There are four main components for managing physical security that are widely accepted across both civilian and military organisations, known as DDDR:

- Deterrence
- Detection
- Delay
- Response

Recovery can also be included as a last step in the process.

Deterrence is designed to convince the potential attacker that a successful attempt is likely to be thwarted. Deterrence methods usually include physical barriers, walls, fences, signage and lighting. Location and design also play a role in protecting the asset. Alarm systems and guards are also a key element in visibly highlighting the level of deterrence.

Access controls are an important element for deterrence. This includes Personnel ID management, gates, doors, locks and electronic access controls for data protection. Policies and procedures are a requirement for setting the organisations expectations and guidelines.

Detection is an important tool for monitoring physical sites and systems and recording any activity that occurs. Surveillance is essential at every level of the four components.

Delay is preferable, particularly for physical sites, where preventing the perpetrators from completing their act is desirable. Slowing an attack-in-progress can also allow the organisation to respond before assets are compromised.