A Security Systems Installation Project Case Study

an Australian Perspective
By the Numbers

- 28 road tunnels
- 4,121 traffic signals
- 12,847 km² of navigable waterways and 2,137 km of coastline
- 24,084 commercial and private boat moorings & 3,873 maritime navigational aids
- 5.4 million licenced car drivers
- 6.5 million registered vehicles
- 4.3 million people cross the Sydney Harbour Bridge and Tunnel by car, bus and train every week
- 500,000 licensed boat drivers and 225,000 vessels
- A Sydney road network that supports nearly 12 million journeys each day

GSX.org | #GSX18

SOLUTIONS MULTIPLIED.
Australia/USA Comparison

NSW - 309,000 sq. miles
- 47 x Hawaii’s
- 5 x Florida’s
- 2 x California’s
- 1 x Texas
Kangaroo Lesson #1

Myths about Australia
Security & Critical Infrastructure Resilience

BACKGROUND

• The Security & Critical Infrastructure Resilience Branch manages the protection of critical transport infrastructure and the provision of security services to RMS

• Critical Infrastructure sites are those listed at State and Commonwealth level as having significant economic, social or national security importance to the nation

• Currently monitoring 20+ Critical Infrastructure sites across NSW

• The S&CIR Program enables transport network resilience through the prevention, preparation, response and recovery from adverse events impacting on these assets
Security & Critical Infrastructure Resilience

BACKGROUND

• Transport Modes within the transport cluster are broken down into:
  • 53% Rail - 42% Bus - 3% Ferries - 2% Light Rail
  • 100% Road

• Road Infrastructure accounts for 100%, in the operations of the other Critical Infrastructure services such as food, water, energy, transport, telecommunication and health

• The National Terrorism Threat Advisory Level is currently set at PROBABLE by the Australian Security Intelligence Organisation (ASIO) indicating a terrorist attack is likely
Security Landscape

THE AUSTRALIAN ENVIRONMENT

• First ‘Terrorist Attack’ in Australia was in 1915
• 7 x Significant Bombings
• 2 x Active Shooter Events
• 3 x Stabbing Attacks
• 2 x Sieges
• 4 x Assassinations
Security Landscape

THE AUSTRALIAN ENVIRONMENT

- Plots Foiled
  - 2 x Assassination
  - 5 x Bombing
  - 1 x Designer
  - 13 x Active Shooter
Critical Infrastructure Assessments

RESILIENCE -v- PROTECTION

Critical Infrastructure Resilience
-the capacity of CI to withstand disruption, operate effectively in crisis, and
deal with and adapt to shocks and stresses. It includes the flexibility to
adapt to present and future conditions

Critical Infrastructure Protection
-minimises vulnerability to criminal or malicious threats via physical,
procedural, person-based, and electronic defences. Critical Infrastructure
Protection is a key part of Critical Infrastructure Resilience
Critical Infrastructure Assessments

01 IDENTIFICATION OF CRITICAL INFRASTRUCTURE
NSW CI assets identified through sector meetings

02 DETERMINATION OF CRITICALITY RATING
NSW CI Panel review & confirm CI Asset and Criticality Rating

03 UNDERSTAND THREAT AND HAZARD

04 CONDUCT RISK AND VULNERABILITY ASSESSMENT

05 MANAGE IDENTIFIED RISKS (Risk Management Actions)

06 UNDERTAKE PLANNING, EXERCISING, EVALUATION AND REVIEW

PROCESS OCCURS PRIOR TO CI PROTECTION PROCESS
Critical Infrastructure Assessments

DEFINING CRITICAL INFRASTRUCTURE

- What is and is not CI
- Measurable & Quantifiable
- Scalable & Responsive

Shopping Centre Underpass

Bus Interchange 18 x Pedestrian Lifts

Pedestrian Tunnel Transit Way

Cycleway Underpass Roundabout
Critical Infrastructure Assessments

THE INTEGRITY OF THE PROCESS

• Survivability of the Asset
  • Death and Injury

• What you are Protecting

• Calling out all of the details

• Provide Options & Priorities

• Honesty

• Use Experts

• Assess & Reassess
Critical Infrastructure Assessments

CONFIDENTIALITY & INFORMATION

- Investigation / Assessment
- Reports
- Data
- Open Source
- Imagery
- Signature
Kangaroo Lesson #2

Kangaroo’s in the Workplace
Critical Infrastructure Assessments

THE DETAIL

• Site Details
  • Formal Detail
    • Owner
    • Operator
    • Designation
  • Location
  • Maps
  • History
  • Background

• Specifics
  • Road Length, Lanes, Directions
  • Tunnel Height
  • River Width
Critical Infrastructure Assessments

THE DETAIL

• Scope
  • What is in and out of scope
• Previous Assessments
• Asset Functions & Utilisation
  • Maintenance Requirements
  • Traffic Modelling & Social Impact
• Criticality & Iconic Status

• Local Area & Topography
  • Roads & Local Area
    • Flood Plains
  • Utilities
Critical Infrastructure Assessments

THE DETAIL

• Construction Details
  • Construction Methods
    • Concrete Density
  • Power (HV), Substations
    • Feeds
    • Switch Rooms
    • Remote Switching (Security)
  • Communications Systems
    • Radio
    • RRB
  • Lighting

• Access Points
• Underground Layouts
  • Internal
  • External
Critical Infrastructure Assessments

THE DETAIL

• Construction Details (cont.)
  • ITS
    • Road Loops
    • VMS
    • Camera’s (Speed, ANPR, Rest)
    • Traffic Detection
    • OHVD
  • Maintenance Monitoring
  • Life Safety Systems
  • Security Systems
    • Control Rooms, CCTV, Guarding

• Technologies
  • Servers
  • UPS
  • Fibre (Redundancies)
  • Wi-Fi & Security
Critical Infrastructure Assessments

THE DETAIL

• Construction Details (cont.)
  • Fire Safety Systems
  • Roadways & Access
    • Rights
    • Alternatives
    • Neighbours
  • Exhaust/Intakes
  • HVAC
  • Unique Systems
Critical Infrastructure Assessments

THE DETAIL

• Emergency Systems
  • Evacuation
    • Plans
    • Diagrams
      • Road/Tunnel Users
      • Staff
      • Contractors & Visitors
    • Exercises (Recency)
  • Incident Management Systems
  • Spill Management

• Fire
  • Water Sources
  • Responders
  • Foam
Critical Infrastructure Assessments

THE DETAIL

• Emergency Systems (cont.)
  • Detection
  • Suppression
  • Emergency Services Familiarisation
    • Local Police Responders
    • Fire, Ambulance
    • Negotiators
    • Rescue
    • Sniper & Counter Sniper
    • Specials
  • Environmental Detection
    • CO2

• Public Address Systems
  • Testing Regime
• Entry/Exit Overrides
• Dangerous Goods Storage
• HAZMAT & HAZCHEM
• Panels
  • Locations
  • Access
  • Mimic
Critical Infrastructure Assessments

THE DETAIL

- Security Systems
  - Access Control
  - Fencing & Perimeter
  - Cameras
    - Locations
    - Diagrams
    - Access
  - Intelligence & Incident Reports
    - Administrative Security
  - Security & Response Plans
    - Evacuations
  - Resilience Integration

- CCTV System
  - VMS
  - Servers
  - Cabling
  - Remote Access

- Security
  - Information
  - Access Control
  - Storage
  - External Connection
Critical Infrastructure Assessments

THE DETAIL

• Dependencies & Interdependencies
  • Government Departments
  • Businesses
  • Transport Hubs
  • Heavy Vehicle Routes
  • Stakeholders
  • Legislative
  • Local Area
  • Combat Agencies
Critical Infrastructure Assessments

TREATMENTS & RECOMMENDATIONS

- Standard Treatments
  - Barriers, Fences & Bollards
  - CCTV & Guarding
  - Motion Detection
  - Lighting.

- Site Specific Treatments
  - Training
  - Procedures
  - Incident Procedures
  - Drills & Exercises

- Behavioural Treatments
  - Staff Security
  - Security Culture
  - Westminster Bridge Analysis

- Proactive Treatments
  - ANPR
  - Facial Recognition
  - Movement Analysis

- Review
Critical Infrastructure Assessments

SUPPORTING DOCUMENTATION

- Threat List & Methods of Delivery
- Likelihood Analysis Matrix
- Likelihood Analysis Table
- Consequence Analysis Matrix
- Consequence Analysis Table
- Security & Threat Assessment Matrix
Kangaroo Lesson #3

Kangaroo’s & Sport
## Risk Matrix

<table>
<thead>
<tr>
<th>Likelihood</th>
<th>Negligible impact</th>
<th>Some impact, adverse results</th>
<th>Impacts begin to change the ability to maintain normal operations</th>
<th>Likely to have significant impact</th>
<th>High-probability risk likely to have an extended impact.</th>
<th>Sudden disaster of immense proportions that has severe consequences, often accompanied by destruction of assets and/or loss of life.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Insignificant</td>
<td>Minor</td>
<td>Moderate</td>
<td>Major</td>
<td>Severe</td>
<td>Catastrophic</td>
<td></td>
</tr>
<tr>
<td>The risk with assigned consequence could occur multiple times (&gt;10) during any given year.</td>
<td>Almost certain</td>
<td>Medium</td>
<td>High</td>
<td>High</td>
<td>Very High</td>
<td>Very High</td>
</tr>
<tr>
<td>The risk with assigned consequence could occur occasionally (&lt;10) during any given year.</td>
<td>Very likely</td>
<td>Medium</td>
<td>Medium</td>
<td>High</td>
<td>High</td>
<td>Very High</td>
</tr>
<tr>
<td>The risk with assigned consequence could occur once during any given year.</td>
<td>Likely</td>
<td>Low</td>
<td>Medium</td>
<td>Medium</td>
<td>High</td>
<td>High</td>
</tr>
<tr>
<td>The risk with assigned consequence could occur once over 10 years.</td>
<td>Unlikely</td>
<td>Low</td>
<td>Low</td>
<td>Medium</td>
<td>Medium</td>
<td>High</td>
</tr>
<tr>
<td>The risk with assigned consequence could occur once in the next 100 years.</td>
<td>Very unlikely</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Medium</td>
<td>Medium</td>
</tr>
<tr>
<td>The risk with assigned consequence is not expected to occur in the next 100 years.</td>
<td>Almost unprecedented</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Low</td>
<td>Medium</td>
</tr>
<tr>
<td>Level</td>
<td>Likelihood</td>
<td>Semi-Quantitive</td>
<td>Quantitative</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>-------</td>
<td>--------------------</td>
<td>----------------------------------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
| 1     | Almost Unprecedented | The risk with assigned consequence is not expected to occur in the next 100 years. | • There is very little or no real chance of this risk occurring.  
• History shows that this risk hardly ever happens, if at all.  
• We have a high level of confidence and faith in the controls to prevent the risk.  
• Everyone would be shocked and surprised if this risk occurs.  
• No reasonable person would ever consider that the risk could occur.  
• No one would have seen this risk coming. |
|       |                    | The risk with assigned consequence may occur less than 1 in 10,000 times (if ever) the event or action occurs. I.E. < 0.01% chance of occurrence. |                                                                             |
| 2     | Very Unlikely      | The risk with assigned consequence could occur once in the next 100 years.        | • There is only an unusual chance of this risk occurring.  
• History shows that this risk rarely happens, usually under unusual circumstances.  
• We have a strong level of confidence that the controls will prevent the risk.  
• Most staff would understand the risk could happen but would still be surprised.  
• Most reasonable people would consider it rare or unusual for the risk to occur.  
• You can be forgiven for not anticipating the risk was about to occur. |
|       |                    | The risk with assigned consequence could occur between 1 in 1,000 and 1 in 10,000 times the event or action occurs. I.E. 0.01% to 0.1% chance of occurrence. |                                                                             |
| 3     | Unlikely           | The risk with assigned consequence could occur once over 10 years.                | • There is a chance of this risk occurring but not very often.  
• History shows that this risk does happen but not very frequently.  
• We have a reasonable level of confidence that the controls will prevent the risk.  
• Most staff while surprised, would not be shocked if this risk occurs.  
• Most reasonable people would have expected the risk to occur at some time.  
• You should have been anticipating the risk. |
|       |                    | The risk with assigned consequence is expected to occur between 1 in 100 and 1 in 1,000 times the event or action occurs. I.E. 0.1% to 1% chance of occurrence. |                                                                             |
| 4     | Likely             | The risk with assigned consequence could occur once during any given year.         | • There is a chance of this risk occurring in the current period.  
• History shows that the risk has occurred on a number of occasions.  
• Moderate confidence in the controls, may not work under certain circumstances.  
• Most staff would have considered the risk was possible.  
• Most reasonable people would have expected it to occur.  
• You should have been watching/monitoring for this risk to occur. |
|       |                    | The risk with assigned consequence could occur between 1 in 10 and 1 in 100 times the event or action occurs. I.E. 1% to 10% chance of occurrence. |                                                                             |
| 5     | Very Likely        | The risk with assigned consequence could occur occasionally (<10) during any given year. | • There is a good chance of this risk occurring.  
• History shows that the risk occurs unacceptably too often.  
• Controls may help prevent its occurrence but wouldn’t rely heavily on them.  
• Most staff would not be surprised if and when the risk occurs.  
• Most reasonable people would have expected it to occur on a semi regular basis.  
• You should have expected this risk to occur. |
|       |                    | The risk with assigned consequence could occur between 1 in 4 and 1 in 10 times the event or action occurs. I.E. 10% to 25% chance of occurrence. |                                                                             |
| 6     | Almost Certain     | The risk with assigned consequence could occur multiple times (>10) during any given year. | • There is a very strong chance of this risk occurring.  
• History shows that it is something that occurs frequently.  
• We have little or no faith in the controls to prevent its occurrence.  
• No one will be surprised if and when the risk occurs – in fact it’s expected to.  
• A reasonable person would consider it obvious and certain that the risk would occur.  
• You should have seen this risk coming. |
<p>|       |                    | The risk with assigned consequence could occur at least 1 in every 4 times the event or action occurs I.E. &gt; 25% chance of occurrence. This risk is known to occur frequently. |                                                                             |</p>
<table>
<thead>
<tr>
<th>Impact</th>
<th>Details</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Catastrophic</td>
<td>Immediate reportable and/or explanation required</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Severe</td>
<td>Some isolated cancellation of events to a major culturally important community event</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Moderate</td>
<td>Minor delay to a culturally important community event</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Minor</td>
<td>Temporary cancellation or significant delay to a major culturally important community event</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Insignificant</td>
<td>No permanent dispersal</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Impact</th>
<th>Details</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Catastrophic</td>
<td>Deaths greater than 1 in 1,000 people for the population of interest</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Severe</td>
<td>Loss in economic activity and/or asset value</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Moderate</td>
<td>Minor injuries or illnesses resulting in lost time</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Minor</td>
<td>No discernible impact, benefit realisation largely intact</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Insignificant</td>
<td>Errors, incidents occur occasionally and some ‘annoying’ inefficiencies exist that partially impact operations</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Impact</th>
<th>Details</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Catastrophic</td>
<td>Significant loss or impairment of an ecosystem or species recognised at the state level</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Severe</td>
<td>Significant external resources required to return the community to normal function</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Moderate</td>
<td>Minor breach of contract by either party rectified through local management discussion</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Minor</td>
<td>Employee morale is low</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Insignificant</td>
<td>Errors, omissions, incidents occurring on a regular basis due to poor controls</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Impact</th>
<th>Details</th>
<th>Description</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Catastrophic</td>
<td>Significant industry or business sector is significantly impacted by the emergency event, resulting in operations impairing operational performance and delaying outcomes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Severe</td>
<td>The Chief Executive and/or multiple RMS Executives relieved of duty with external ‘caretaker’ appointed.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Moderate</td>
<td>Staff and service availability impacted by absence of union effort to support the Program go ahead</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Minor</td>
<td>Revenue, OPEX or non-infrastructure CAPEX impact &lt; $100K</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Insignificant</td>
<td>Revenue, OPEX or non-infrastructure CAPEX impact &gt; $50M</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

GSX.org | #GSX18
Critical Infrastructure Assessments

RISK MATRIX - CONSEQUENCE

• STATE
  • Economic Activity
  • Industry

• ENVIRONMENT
  • Environmental
  • Species & Ecosystems

• SOCIAL
  • Community Wellbeing
  • Community Services
  • Cultural Activities
  • Cultural Objects

• PEOPLE
  • Mortality
  • Injuries & Illness

• BUSINESS
  • Financial
  • Project/Program
  • Service Delivery
  • Policy & Contract Compliance
  • Reputation (Confidence)
  • External Stakeholder Intervention
  • WHS
  • Employees
  • Governance & Control
Critical Infrastructure Assessments

THREATS

- Active Armed Offender (Firearm)
- Active Armed Offender (Basic Weapon)
- Accidental Impact
- Aircraft
- Arson / Fire Bomb
- Communicated Threat
- Concerted Ill Discipline
- Crude CBRN
- Crude Cyber
- Demonstration
- Hostile Vehicle/Vessel
- Natural Disaster
- Malicious Damage
- PBIED
- PIED
- RPAS
- Sabotage
- Siege & Hostage
- Sophisticated CBRN
- Sophisticated Cyber
- Supply Interruption
- Trusted Insider
- VhBIEED
- VsBIEED
Critical Infrastructure Assessments

LIKELIHOOD v PERCEPTION TEST

• **Is Paul getting Drunk on Thursday Night?**
  • Do I drink?
  • How hard is it to get a drink?
  • What times and are there restrictions on drinking?
  • What are the Size and Types of the Drinks?
  • What is the Alcohol Content?
  • What is my favourite Drink?
  • Do I have enough Money?
  • Will I be alone and are there triggers?
  • What is the frequency of me getting Drunk?
  • How do you measure that?
## Critical Infrastructure Assessments

### LIKELIHOOD ANALYSIS MATRIX

<table>
<thead>
<tr>
<th>MATERIALS ATTAINABILITY</th>
<th>OPERATIONAL EASE</th>
<th>EASE OF RECONNAISSANCE</th>
<th>THREAT ATTRACTIVENESS</th>
</tr>
</thead>
<tbody>
<tr>
<td>GRADE</td>
<td>GRADE</td>
<td>GRADE</td>
<td>GRADE</td>
</tr>
</tbody>
</table>

**Materials Attainability**
- Grades range from Very Easy to Very Difficult (1-5).
- Examples: None, Easy, Moderate, Complex.

**Operational Ease**
- Grades range from Very Basic to Very Complex (1-5).
- Examples: Basic, Composite, Very Complex.

**Ease of Reconnaissance**
- Grades range from No Information Required to Very Detailed Information Required (1-6).
- Examples: No Information Required, Basic, Detailed.

**Threat Attractiveness**
- Grades range from Unattractive to Highly Attractive (1-5).
- Examples: Unattractive, Basic, Complex.

The table above illustrates the likelihood of various attacks on critical infrastructure. Each column represents a different aspect of the assessment, with grades indicating the level of ease or difficulty. This framework helps in understanding the potential risks and vulnerabilities associated with infrastructure threats.
Critical Infrastructure Assessments

MATERIAL AVAILABILITY

• How easy is it to obtain?
  • Edged Weapons
  • Firearms
  • Explosives
  • Chemicals
  • Trucks
• How easy is it to be detected?
• What is required for storage?

• Who makes the decision on Material Availability?
  • Industry Variants
  • Targeting supplies and suppliers
# Critical Infrastructure Assessments

## LIKELIHOOD ANALYSIS MATRIX

### MATERIALS ATTAINABILITY

The ease with which the explosives, devices, weapons or other objects required to carry out the attack according to the level of the presumed actual accessibility in NSW at the time of the assessment.

<table>
<thead>
<tr>
<th>GRADE</th>
<th>Attainability</th>
</tr>
</thead>
<tbody>
<tr>
<td>Very Easy (10)</td>
<td>The object or parts can be obtained easily</td>
</tr>
<tr>
<td>Somewhat Easy  (7 - 9)</td>
<td></td>
</tr>
<tr>
<td>Problematic (4 - 6)</td>
<td></td>
</tr>
<tr>
<td>Difficult (1 - 3)</td>
<td></td>
</tr>
<tr>
<td>Very Difficult (0)</td>
<td></td>
</tr>
</tbody>
</table>

### OPERATIONAL EASE

Evaluates the skills, situations and the environment a terrorist needs in order to plan and successfully execute each threat to the facility. This relates to the ease in which the specific threat analysed, within the context of the security/complexity and structure, allows an attack at each location under review.

<table>
<thead>
<tr>
<th>GRADE</th>
<th>Security</th>
<th>GRADE</th>
<th>Device Complexity</th>
<th>GRADE</th>
<th>Site Structure</th>
</tr>
</thead>
<tbody>
<tr>
<td>None (10)</td>
<td></td>
<td>Very Basic (10)</td>
<td></td>
<td>No Restriction (10)</td>
<td></td>
</tr>
<tr>
<td>Ineffective (7 - 9)</td>
<td></td>
<td>Somewhat Basic (7 - 9)</td>
<td></td>
<td>Easy (7 - 9)</td>
<td></td>
</tr>
<tr>
<td>Basic (4 - 6)</td>
<td></td>
<td>Basic (4 - 6)</td>
<td></td>
<td>Restrictive (4 - 6)</td>
<td></td>
</tr>
<tr>
<td>Effective (1 - 3)</td>
<td></td>
<td>Complex (1 - 3)</td>
<td></td>
<td>Somewhat Restrictive (1 - 3)</td>
<td></td>
</tr>
<tr>
<td>Very Effective (0)</td>
<td></td>
<td>Very Complex (0)</td>
<td></td>
<td>Very Restrictive (0)</td>
<td></td>
</tr>
</tbody>
</table>
### Critical Infrastructure Assessments

#### LIKELIHOOD ANALYSIS MATRIX

<table>
<thead>
<tr>
<th>EASE OF RECONNAISSANCE</th>
<th>THREAT ATTRACTIVENESS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>GRADE</strong></td>
<td><strong>THREAT METHOD FACTOR</strong></td>
</tr>
<tr>
<td>No Information Required (10)</td>
<td>Highly Attractive (10)</td>
</tr>
<tr>
<td>Little Information Required (7 - 9)</td>
<td>Attractive (7 - 9)</td>
</tr>
<tr>
<td>Basic Information Required (4 - 6)</td>
<td>Problematic (4 - 6)</td>
</tr>
<tr>
<td>Detailed Information Req (1 - 3)</td>
<td>Difficult (1 - 3)</td>
</tr>
<tr>
<td>Very Detailed Information Req (0)</td>
<td>Very Difficult (0)</td>
</tr>
</tbody>
</table>

#### EASE OF RECONNAISSANCE
- **Need for Information**: The information required to successfully carry out an attack including the structure and operations of the facility along with the requirements and instructions to build a device or obtaining the object and/or parts.
- **Ease of Obtaining**: Open Source Reporting, Common Knowledge, Details of any Facility Vulnerability, Experience of Attacker / Group (e.g. site plans available on the internet).

#### THREAT ATTRACTIVENESS
- **Threat Preference (RTX)**: A rating specifically based on the result of the 'Red Team' Exercise against the facility (e.g. the ease in which access was gained, the impact that interruption might have with information gained during exercise).
- **Threat Method Factor**: The attractiveness of the facility to an attacker to carry out the attack, including the possibility of copying previous attacks and the trends identified by intelligence and incident analysis (e.g. returning foreign fighters, overseas incidents).
## Critical Infrastructure Assessments

### LIKELIHOOD ANALYSIS TABLE

<table>
<thead>
<tr>
<th>THREAT LIST</th>
<th>MATERIALS ATTAINABILITY</th>
<th>OPERATIONAL EASE</th>
<th>EASE OF RECONNAISSANCE</th>
<th>THREAT ATTRACTIVENESS</th>
<th>TOTAL</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Security</td>
<td>Device Complexity</td>
<td>Site Structure</td>
<td>Need for Information</td>
<td>Threat Preference based on RTX</td>
</tr>
<tr>
<td>Abduction / Kidnapping</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Active Armed Offender - Firearms</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Active Armed Offender - Basic Weapon</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Aircraft - Large</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Aircraft - Small</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Arson / Fire Bomb</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Assassination</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Communicated Threat</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Crude Biological</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Crude Chemical</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Crude Cyber</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Crude Radiological</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Hostile Vehicle / Vessel</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Nuclear</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Person Borne IED</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Placed IED</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Riot / Demonstration</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Sabotage</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Siege &amp; Hostage</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Sophisticated Biological</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Sophisticated Chemical</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Sophisticated Cyber</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Sophisticated Radiological</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Vehicle Borne IED</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Vessel Borne IED</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
Critical Infrastructure Assessments

LIKELIHOOD ANALYSIS TABLE

VEHICLE BORNE IED – Targeting Vehicles

MATERIALS ATTAINABILITY

The ingredients for a VBIED can be easily sourced through retail outlets (i.e., Fertiliser, LPG, Chlorine). Explosives, although appearing difficult, can be obtained as has been demonstrated in a number of recent incidents or manufactured such as the incident with the Australian Student in Sydney. Vehicles are also easily obtained and can be brought to the tunnel without detection as there are no access controls for vehicles.

<table>
<thead>
<tr>
<th></th>
<th>GRADE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security</td>
<td>5</td>
</tr>
<tr>
<td>Device Complexity</td>
<td>2</td>
</tr>
<tr>
<td>Site Structure</td>
<td>6</td>
</tr>
</tbody>
</table>

OPERATIONAL EASE

<table>
<thead>
<tr>
<th></th>
<th>GRADE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security</td>
<td>10</td>
</tr>
<tr>
<td>Device Complexity</td>
<td>2</td>
</tr>
<tr>
<td>Site Structure</td>
<td>6</td>
</tr>
</tbody>
</table>

EASE OF RECONNAISSANCE

<table>
<thead>
<tr>
<th></th>
<th>GRADE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Need for Information</td>
<td>4</td>
</tr>
<tr>
<td>Ease of Obtaining</td>
<td>10</td>
</tr>
</tbody>
</table>

THREAT ATTRACTIVENESS

LIKELIHOOD WEIGHTING 25%

<table>
<thead>
<tr>
<th></th>
<th>GRADE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat Preference (RTX)</td>
<td>8</td>
</tr>
<tr>
<td>Threat Method Factor</td>
<td>9</td>
</tr>
</tbody>
</table>

OVERALL GRADE

26.44
Critical Infrastructure Assessments

CONSEQUENCE

• Both Likelihood and Consequence are equal partners in the process
• It can be considered as the driver for the process
• ‘Now What’
• It can assist with prioritising and budget allocation
• Unlike Likelihood, it is not subject to fluctuations
  • There are some inputs subject to change such as traffic flow, costs, interdependencies
### Critical Infrastructure Assessments

#### CONSEQUENCE ANALYSIS MATRIX

<table>
<thead>
<tr>
<th>DAMAGE &amp; OPERATION</th>
<th>IMPACTS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Damage to Asset</td>
<td>Population Exposed and/or Impacted</td>
</tr>
<tr>
<td>Replacement Cost</td>
<td>The Impact on the population in affecting their normal day-to-day activities</td>
</tr>
<tr>
<td>Return to Operation</td>
<td>1 Vital or 6+ Significant</td>
</tr>
<tr>
<td>Corridor Impact</td>
<td>500,000 +</td>
</tr>
<tr>
<td>Expected Return to Operation</td>
<td>14 Days</td>
</tr>
<tr>
<td>Risk to Asset</td>
<td>30,000</td>
</tr>
<tr>
<td>Replacement Cost</td>
<td>No Corridor</td>
</tr>
<tr>
<td>Return to Operation</td>
<td>a period of a few hours to a maximum of 24 Hours</td>
</tr>
<tr>
<td>Corridor Impact</td>
<td>0 - 10,000</td>
</tr>
</tbody>
</table>

### Table Legend

- **Catastrophic** (1-10)
  - Total Loss - Completely destroyed buildings with no possibility of repair
  - Total Loss - Completely destroyed buildings with no possibility of repair
  - Total Loss - Completely destroyed buildings with no possibility of repair
  - Total Loss - Completely destroyed buildings with no possibility of repair
  - Total Loss - Completely destroyed buildings with no possibility of repair
  - Total Loss - Completely destroyed buildings with no possibility of repair
  - Total Loss - Completely destroyed buildings with no possibility of repair
  - Total Loss - Completely destroyed buildings with no possibility of repair
  - Total Loss - Completely destroyed buildings with no possibility of repair
  - Total Loss - Completely destroyed buildings with no possibility of repair

- **Major** (7-8)
  - Moderate (5-6)
  - Minor (3-4)
  - No Significant (0-2)
  - Little or no damage
  - No Corridor
  - No Corridor
  - No Corridor
  - No Corridor
  - No Corridor

- **Risk to Asset**
  - Risk to Asset
  - Risk to Asset
  - Risk to Asset
  - Risk to Asset
  - Risk to Asset
  - Risk to Asset
  - Risk to Asset
  - Risk to Asset
  - Risk to Asset

- **Replacement Cost**
  - Replacement Cost
  - Replacement Cost
  - Replacement Cost
  - Replacement Cost
  - Replacement Cost
  - Replacement Cost
  - Replacement Cost
  - Replacement Cost
  - Replacement Cost

- **Return to Operation**
  - Return to Operation
  - Return to Operation
  - Return to Operation
  - Return to Operation
  - Return to Operation
  - Return to Operation
  - Return to Operation
  - Return to Operation
  - Return to Operation

- **Corridor Impact**
  - Corridor Impact
  - Corridor Impact
  - Corridor Impact
  - Corridor Impact
  - Corridor Impact
  - Corridor Impact
  - Corridor Impact
  - Corridor Impact
  - Corridor Impact

- **IMMEDIATE RESPONSE**
  - IMMEDIATE RESPONSE
  - IMMEDIATE RESPONSE
  - IMMEDIATE RESPONSE
  - IMMEDIATE RESPONSE
  - IMMEDIATE RESPONSE
  - IMMEDIATE RESPONSE
  - IMMEDIATE RESPONSE
  - IMMEDIATE RESPONSE
  - IMMEDIATE RESPONSE

- **POPULATION IMPACT**
  - POPULATION IMPACT
  - POPULATION IMPACT
  - POPULATION IMPACT
  - POPULATION IMPACT
  - POPULATION IMPACT
  - POPULATION IMPACT
  - POPULATION IMPACT
  - POPULATION IMPACT
  - POPULATION IMPACT

- **ECONOMIC IMPACT**
  - ECONOMIC IMPACT
  - ECONOMIC IMPACT
  - ECONOMIC IMPACT
  - ECONOMIC IMPACT
  - ECONOMIC IMPACT
  - ECONOMIC IMPACT
  - ECONOMIC IMPACT
  - ECONOMIC IMPACT
  - ECONOMIC IMPACT

- **MEDIA, SOCIAL IMPACT & SOCIAL DISRUPTION**
  - MEDIA, SOCIAL IMPACT & SOCIAL DISRUPTION
  - MEDIA, SOCIAL IMPACT & SOCIAL DISRUPTION
  - MEDIA, SOCIAL IMPACT & SOCIAL DISRUPTION
  - MEDIA, SOCIAL IMPACT & SOCIAL DISRUPTION
  - MEDIA, SOCIAL IMPACT & SOCIAL DISRUPTION
  - MEDIA, SOCIAL IMPACT & SOCIAL DISRUPTION
  - MEDIA, SOCIAL IMPACT & SOCIAL DISRUPTION
  - MEDIA, SOCIAL IMPACT & SOCIAL DISRUPTION
  - MEDIA, SOCIAL IMPACT & SOCIAL DISRUPTION

- **ENVIRONMENTAL IMPACT (URBAN)**
  - ENVIRONMENTAL IMPACT (URBAN)
  - ENVIRONMENTAL IMPACT (URBAN)
  - ENVIRONMENTAL IMPACT (URBAN)
  - ENVIRONMENTAL IMPACT (URBAN)
  - ENVIRONMENTAL IMPACT (URBAN)
  - ENVIRONMENTAL IMPACT (URBAN)
  - ENVIRONMENTAL IMPACT (URBAN)
  - ENVIRONMENTAL IMPACT (URBAN)
  - ENVIRONMENTAL IMPACT (URBAN)

- **ENVIRONMENTAL IMPACT (NATURAL)**
  - ENVIRONMENTAL IMPACT (NATURAL)
  - ENVIRONMENTAL IMPACT (NATURAL)
  - ENVIRONMENTAL IMPACT (NATURAL)
  - ENVIRONMENTAL IMPACT (NATURAL)
  - ENVIRONMENTAL IMPACT (NATURAL)
  - ENVIRONMENTAL IMPACT (NATURAL)
  - ENVIRONMENTAL IMPACT (NATURAL)
  - ENVIRONMENTAL IMPACT (NATURAL)
  - ENVIRONMENTAL IMPACT (NATURAL)

- **IMPACTS**
  - IMPACTS
  - IMPACTS
  - IMPACTS
  - IMPACTS
  - IMPACTS
  - IMPACTS
  - IMPACTS
  - IMPACTS
  - IMPACTS

- **RECOVERY STRATEGIES**
  - RECOVERY STRATEGIES
  - RECOVERY STRATEGIES
  - RECOVERY STRATEGIES
  - RECOVERY STRATEGIES
  - RECOVERY STRATEGIES
  - RECOVERY STRATEGIES
  - RECOVERY STRATEGIES
  - RECOVERY STRATEGIES
  - RECOVERY STRATEGIES

- **SOLUTIONS MULTIPLIED.**
  - SOLUTIONS MULTIPLIED.
  - SOLUTIONS MULTIPLIED.
  - SOLUTIONS MULTIPLIED.
  - SOLUTIONS MULTIPLIED.
  - SOLUTIONS MULTIPLIED.
  - SOLUTIONS MULTIPLIED.
  - SOLUTIONS MULTIPLIED.
  - SOLUTIONS MULTIPLIED.
  - SOLUTIONS MULTIPLIED.

- **GSX.org | #GSX18**
  - GSX.org | #GSX18
  - GSX.org | #GSX18
  - GSX.org | #GSX18
  - GSX.org | #GSX18
  - GSX.org | #GSX18
  - GSX.org | #GSX18
  - GSX.org | #GSX18
  - GSX.org | #GSX18
  - GSX.org | #GSX18
## Critical Infrastructure Assessments

### CONSEQUENCE ANALYSIS MATRIX

<table>
<thead>
<tr>
<th>Damage to Asset</th>
<th>Replacement Cost</th>
<th>Return to Operation</th>
<th>Corridor Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Catastrophic (9 - 10)</strong></td>
<td>80 - 100%</td>
<td>$500 Million +</td>
<td>+ 14 Days</td>
</tr>
<tr>
<td>Total Loss - Completely destroyed buildings with no possibility of repair.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Major (7 - 8)</strong></td>
<td>60 - 80%</td>
<td>$100 Million to $500 Million</td>
<td>7 - 14 Days</td>
</tr>
<tr>
<td>Extensive critical structural damage to facility</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Moderate (5 - 6)</strong></td>
<td>40 - 60%</td>
<td>$10 Million to $100 Million</td>
<td>3 - 7 Days</td>
</tr>
<tr>
<td>Some structural damage with extensive superficial damage (debris, shattered windows etc.)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Minor (3 - 4)</strong></td>
<td>20 - 40%</td>
<td>$1 Million to $10 Million</td>
<td>1 - 3 Days</td>
</tr>
<tr>
<td>Non-structural damage with some superficial damage (debris etc.)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Insignificant (0 - 2)</strong></td>
<td>0 - 20%</td>
<td>$0 to $1 Million</td>
<td>a period of a few hours to a maximum of 24 Hours</td>
</tr>
<tr>
<td>Little or no damage</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Critical Infrastructure Assessments

### CONSEQUENCE ANALYSIS MATRIX

<table>
<thead>
<tr>
<th>IMPACTS</th>
<th>Population Exposed and/or Impacted</th>
<th>Number of Fatalities and/or Casualties</th>
<th>Dependencies</th>
<th>Economic Impact</th>
<th>Media, Social Impact &amp; Social Disruption</th>
<th>Environmental Impact (Urban)</th>
<th>Environmental Impact (Natural)</th>
</tr>
</thead>
<tbody>
<tr>
<td>500,000 +</td>
<td>Sydney Basin Multiple Regions</td>
<td>200 *</td>
<td>High Fatality Levels High Casualty Levels</td>
<td>1+ Vital or 4+ Majors or 8+ Significant</td>
<td>$1 Billion + Creating a major state economic crisis</td>
<td>Extended Worldwide Coverage, Confidence in Government / Authority by Population non-existent, Population remained confined with little or no activity, Irreversible Brand Damage</td>
<td>Large part of target city affected</td>
</tr>
<tr>
<td>150,000 - 500,000</td>
<td>Regional Level Multiple Local Government Areas</td>
<td>50 - 199</td>
<td>Many Fatalities High Casualty Level</td>
<td>2 - 4 Majors or 6 - 8 Significant</td>
<td>$500 Million to $1 Billion Creating a major level economic loss - affects sectors, industries or people in the immediate and surrounding areas</td>
<td>Some Worldwide Coverage with Extensive National Interest, Confidence and Trust in Government / Authority Severely Damaged, Significant Behavioural Changes within Population with Few Activities and Movements, Significant Brand Damage</td>
<td>Entire section or precinct of city affected</td>
</tr>
<tr>
<td>30,000 - 150,000</td>
<td>Local Government Area Multiple Suburbs</td>
<td>10 - 49</td>
<td>Some Fatalities High Casualty Level</td>
<td>2 Majors or 4 - 6 Significant</td>
<td>$100 Million to $500 Million Creating a moderate level economic loss - affects sectors, industries or people only in the immediate area</td>
<td>National Coverage with Extensive Local Interest, Confidence and Trust in Government / Authority Questioned, Large Behavioural Change within Community with Activities and Movements No Longer Occurring, Some Brand Damage</td>
<td>Stress or behavioural changes on ecosystem</td>
</tr>
<tr>
<td>10,000 - 30,000</td>
<td>Whole Suburb Multiple Streets</td>
<td>4 - 9</td>
<td>Some Fatalities Some Casualties</td>
<td>1 Major or 2 - 4 Significant</td>
<td>$50 Million to $100 Million Local economic loss without major effect on surrounding areas</td>
<td>Local Coverage with some Community Interest, Confidence levels remain with Trust Questioned, Some Behavioural Change with some Activities Affected, Little Brand Damage</td>
<td>Physical or chemical level changes only</td>
</tr>
<tr>
<td>0 - 10,000</td>
<td>Whole Street Multiple Homes</td>
<td>0 - 3</td>
<td>No Fatalities Some Casualties</td>
<td>1 - 2 Significant</td>
<td>$0 - $50 Million Minimal economic impact</td>
<td>Little or No Coverage, Confidence and Trust Remain Unaffected, Normal Behaviour and Activities Continue Unaffected, No Brand Damage</td>
<td>Little or No Impact</td>
</tr>
</tbody>
</table>

---

**Notes:**
- The Impact on the population in affecting their normal day-to-day activities.
- The estimated number of fatalities and injuries are based on a ‘worst case’ scenario.
- What other Critical Infrastructure or Utilities Depend on this Facility divided into Vital (Communications, Power), Major (Water, Transport) and Significant (Business Operations, Community Facilities).
- Level of direct and non direct loss due to the facility not in operation.
- Social impact caused by fear, anxiety & stress including behavioural changes such as people not using public transport, not going to work in the CBD, changing their normal behaviour.
- The the impact on the urban (surrounding buildings & infrastructure) environment, depending on the type and location of the attack.
- The impact on the natural environment.
### Critical Infrastructure Assessments

#### CONSEQUENCE ANALYSIS TABLE

#### CRITICAL INFRASTRUCTURE CONSEQUENCE ANALYSIS - LOCATION

<table>
<thead>
<tr>
<th>THREAT</th>
<th>Damage to Asset</th>
<th>Replacement Cost</th>
<th>Return to Operation</th>
<th>Corridor Impact</th>
<th>TOTAL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Armed Offender - Firearms</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Active Armed Offender - Basic Weapon</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Accidental Impact</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Aircraft</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Arson / Fire Bomb</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Communicated Threat</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Conmitted W Discipline</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Crude CBRN</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Crude Cyber</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Crime / Demonstration</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Hostile Vehicle / Vessel</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Natural Disaster</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Malicious Damage</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Person Borne IED - Destruction of Facility</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Person Borne IED - Targeting Vehicles</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Placed IED - Destruction of Facility</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Placed IED - Targeting Vehicles</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Prox: Demonstration</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>RPAS</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Sabotage</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Siege &amp; Frontline</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Sophisticated CBRN</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Sophisticated Cyber</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Supply Interruption</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Trusted Insider</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Vehicle Borne IED - Destruction of Facility</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Vehicle Borne IED - Targeting Vehicles</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Vessel Borne IED - Destruction of Facility</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Vessel Borne IED - Targeting Vessels</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
# Critical Infrastructure Assessments

## ASSESSMENT TABLE - BASIC

<table>
<thead>
<tr>
<th>THREAT LIST</th>
<th>SUB LIST</th>
<th>LIKELIHOOD GRADE</th>
<th>CONSEQUENCE GRADE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Armed Offender - Firearm</td>
<td>1</td>
<td>29</td>
<td></td>
</tr>
<tr>
<td>Active Armed Offender - Basic Weapon</td>
<td>2</td>
<td>28</td>
<td></td>
</tr>
<tr>
<td>Accidental Impact</td>
<td>3</td>
<td>27</td>
<td></td>
</tr>
<tr>
<td>Aircraft</td>
<td>4</td>
<td>26</td>
<td></td>
</tr>
<tr>
<td>Arson / Fire Bomb</td>
<td>5</td>
<td>25</td>
<td></td>
</tr>
<tr>
<td>Communicated Threat</td>
<td>6</td>
<td>24</td>
<td></td>
</tr>
<tr>
<td>Concerted Ill Discipline</td>
<td>7</td>
<td>23</td>
<td></td>
</tr>
<tr>
<td>Crude CBRN</td>
<td>8</td>
<td>22</td>
<td></td>
</tr>
<tr>
<td>Crude Cyber</td>
<td>9</td>
<td>21</td>
<td></td>
</tr>
<tr>
<td>Demonstration</td>
<td>10</td>
<td>20</td>
<td></td>
</tr>
<tr>
<td>Hostile Vehicle / Vessel</td>
<td>11</td>
<td>19</td>
<td></td>
</tr>
<tr>
<td>Natural Disaster</td>
<td>12</td>
<td>18</td>
<td></td>
</tr>
<tr>
<td>Malicious Damage</td>
<td>13</td>
<td>17</td>
<td></td>
</tr>
<tr>
<td>Person Borne IED - Destruction of Facility</td>
<td>14</td>
<td>16</td>
<td></td>
</tr>
<tr>
<td>Person Borne IED - Targeting Vehicles</td>
<td>15</td>
<td>15</td>
<td></td>
</tr>
<tr>
<td>Placed IED - Destruction of Facility</td>
<td>16</td>
<td>14</td>
<td></td>
</tr>
<tr>
<td>Placed IED - Targeting Vehicles</td>
<td>17</td>
<td>13</td>
<td></td>
</tr>
<tr>
<td>Riot / Demonstration</td>
<td>18</td>
<td>12</td>
<td></td>
</tr>
<tr>
<td>RPAS</td>
<td>19</td>
<td>11</td>
<td></td>
</tr>
<tr>
<td>Sabotage</td>
<td>20</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>Siege &amp; Hostage</td>
<td>21</td>
<td>9</td>
<td></td>
</tr>
<tr>
<td>Sophisticated CBRN</td>
<td>22</td>
<td>8</td>
<td></td>
</tr>
<tr>
<td>Sophisticated Cyber</td>
<td>23</td>
<td>7</td>
<td></td>
</tr>
<tr>
<td>Supply Interruption</td>
<td>24</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>Trusted Insider</td>
<td>25</td>
<td>5</td>
<td></td>
</tr>
<tr>
<td>Vehicle Borne IED - Destruction of Facility</td>
<td>26</td>
<td>4</td>
<td></td>
</tr>
<tr>
<td>Vehicle Borne IED - Targeting Vehicles</td>
<td>27</td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>Vessel Borne IED - Destruction of Facility</td>
<td>28</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>Vessel Borne IED - Targeting Vessels</td>
<td>29</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>
# Critical Infrastructure Assessments

## ASSESSMENT TABLE - LOCATION

<table>
<thead>
<tr>
<th>Threat List</th>
<th>Sub List</th>
<th>Likelihood Grade</th>
<th>Consequence Grade</th>
</tr>
</thead>
<tbody>
<tr>
<td>Abduction / Kidnapping</td>
<td></td>
<td>26.6</td>
<td>9.6</td>
</tr>
<tr>
<td>Active Armed Offender - Firearm</td>
<td></td>
<td>33.4</td>
<td>17.0</td>
</tr>
<tr>
<td>Active Armed Offender - Basic Weapon</td>
<td></td>
<td>39.1</td>
<td>14.6</td>
</tr>
<tr>
<td>Aircraft - Large</td>
<td></td>
<td>19.6</td>
<td>36.9</td>
</tr>
<tr>
<td>Aircraft - Small</td>
<td></td>
<td>27.1</td>
<td>29.6</td>
</tr>
<tr>
<td>Arson / Fire Bomb</td>
<td></td>
<td>27.1</td>
<td>25.8</td>
</tr>
<tr>
<td>Assassination</td>
<td></td>
<td>24.1</td>
<td>12.0</td>
</tr>
<tr>
<td>Communicated Threat</td>
<td></td>
<td>33.1</td>
<td>9.0</td>
</tr>
<tr>
<td>Crude Biological</td>
<td></td>
<td>21.0</td>
<td>15.3</td>
</tr>
<tr>
<td>Crude Chemical</td>
<td></td>
<td>21.5</td>
<td>20.1</td>
</tr>
<tr>
<td>Crude Cyber</td>
<td></td>
<td>17.3</td>
<td>10.9</td>
</tr>
<tr>
<td>Crude Radiological</td>
<td></td>
<td>19.0</td>
<td>26.1</td>
</tr>
<tr>
<td>Hostile Vehicle / Vessel</td>
<td></td>
<td>35.8</td>
<td>24.3</td>
</tr>
<tr>
<td>Nuclear</td>
<td></td>
<td>7.9</td>
<td>40.0</td>
</tr>
<tr>
<td>PBIED (Collapse of Tunnel)</td>
<td></td>
<td>19.1</td>
<td>32.5</td>
</tr>
<tr>
<td>PBIED (Targeting Vehicles)</td>
<td></td>
<td>23.0</td>
<td>22.7</td>
</tr>
<tr>
<td>PIED (Collapse of Tunnel)</td>
<td></td>
<td>21.3</td>
<td>33.3</td>
</tr>
<tr>
<td>PIED (Targeting Vehicles)</td>
<td></td>
<td>26.6</td>
<td>24.5</td>
</tr>
<tr>
<td>Riot / Demonstration</td>
<td></td>
<td>23.8</td>
<td>13.1</td>
</tr>
<tr>
<td>Sabotage</td>
<td></td>
<td>19.5</td>
<td>17.6</td>
</tr>
<tr>
<td>Siege &amp; Hostage</td>
<td></td>
<td>31.6</td>
<td>14.6</td>
</tr>
<tr>
<td>Sophisticated Biological</td>
<td></td>
<td>10.0</td>
<td>19.1</td>
</tr>
<tr>
<td>Sophisticated Chemical</td>
<td></td>
<td>11.5</td>
<td>25.4</td>
</tr>
<tr>
<td>Sophisticated Cyber</td>
<td></td>
<td>11.5</td>
<td>13.1</td>
</tr>
<tr>
<td>Sophisticated Radiological</td>
<td></td>
<td>6.8</td>
<td>32.9</td>
</tr>
<tr>
<td>VBIED (Collapse of Tunnel)</td>
<td></td>
<td>19.3</td>
<td>33.5</td>
</tr>
<tr>
<td>VBIED (Targeting Vehicles)</td>
<td></td>
<td>26.4</td>
<td>30.1</td>
</tr>
<tr>
<td>VIED</td>
<td></td>
<td>0.0</td>
<td>0.0</td>
</tr>
</tbody>
</table>
Kangaroo Lesson #3

How to Deal with a Kangaroo
Project Case Study

BACKGROUND

• Threat & Security Assessments were carried out at each location and as a result, 60% of cameras originally planned were removed and the new cameras placed in new positions to provide better coverage.

• The assessment also included the maintenance aspects of each installation along with the removal of EWP’s as part of the maintenance and installation process.

• The tender’s technical requirements were very specific, resulting in a small number of cameras meeting the requirements. The scope was changed to provide the industry with performance standards (not technical) to encourage competition, driving down price.
Project Case Study

TENDER SELECTION

• Price & Value for Money
• Service Delivery, Service Provider Experience and Competency
• Implementation of Works, Minimised Operational Risk and Disruption
• Quality of Systems, Policies and Procedures
• Technical Detail and Equipment
• Compliance with Documentation
• Innovation & Value Added Proposals responding to the Scope of Works
• Sustainability Practices in delivering the Scope of Works
Project Case Study

KEY ISSUES

• The major challenge was its predefined and narrow scope.

• Before starting the tender process for Stage 2, a review of Stage 1 was conducted and as a result, the scope for Stage 2 was amended.

• A full review was conducted including interviews with the Security Operations Manager, Operating Assets & Security Manager, the Tenderer, Contractors & Sub Contractors and Control Room Operators. The project was re-scoped and re-budgeted as a result.

• Confidentiality was also an important consideration, although there were non-disclosure agreements in place, the information was released in stages as the tendering process progressed.
There was also no industry engagement, it was left to a remote and sterile tender process.

Site visits were arranged with interested tenderers and a presentation provided for all tenderers 4 weeks prior to tender closing for questions and clarifications.

The engagement with tenderers also resulted in a number of alternate proposals that generated new and emerging technologies that were not specified in the original tender.

Technical Drawing's did not exist.
Project Case Study

CONTRACT

• The contract was amended to include:
  • The introduction of Value Added Proposals and Innovations to the assessment criteria, to drive those efficiencies.
  • Introduction of Sustainability as criteria for assessment, to promote the RMS focus on Environment and Sustainability Strategies.
  • A Monthly Contract Performance Meeting was introduced and formed part of the contractual requirements. This required all invoices for the previous month were required for presentation and approval with only invoices paid from that month.
  • Previous invoices were not accepted with the aim to ensure accurate financial tracking and projections.
Parameters for the measurement of KPI’s which included an overall score and a minimum standard applied to each KPI so substandard performance in one, was not artificially raised by an average across the board.

Adding ‘Asset Tagging’ to the contract to allow for projections for replacement and upgrades over the life of the cameras and the start of an asset register of assets.
## Project Case Study

**CONTRACT CONT.**

<table>
<thead>
<tr>
<th>KPI: Feedback provided by RMS Staff</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>MEASURE:</strong></td>
</tr>
<tr>
<td>1. The number of complaints received against the performance of the Service Provider by RMS Staff, other Contractors or the general public.</td>
</tr>
<tr>
<td>2. The general performance of the Service Provider’s Personnel in day to day operations including presentation and ability to undertake all required tasks.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>ISSUE NUMBER</th>
<th>DETAILS</th>
<th>ECS POSITION</th>
<th>ACTIONS REQUIRED</th>
<th>CLOSED</th>
<th>OPEN</th>
<th>IN DISPUTE</th>
<th>SCORE</th>
<th>RATING</th>
</tr>
</thead>
<tbody>
<tr>
<td>05.01</td>
<td>09002018 - Feedback received from Phil Brooks, RMS Operating Assets and Security Manager, that during the meeting on 03002018 he had been impressed with the speed of the invoicing, the detail and the professional way that the process was being managed by ECS</td>
<td>Nil</td>
<td>Thank RMS for the feedback</td>
<td>CLOSED</td>
<td>3</td>
<td>GOOD</td>
<td></td>
<td></td>
</tr>
<tr>
<td>05.02</td>
<td>11072016 - Feedback received from Control Room that some sub-contractors had attended a site (Gladstone) without appropriate PPE</td>
<td>Nil</td>
<td>Sub Contractors reminded of their responsibilities and a tool box talk issued to all staff to further enforce the requirements for PPE</td>
<td>CLOSED</td>
<td>2</td>
<td>ADEQUATE</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Project Case Study

SAFETY

• Relocating Cameras removing the use of EWP for cleaning and servicing reducing exposure to incidents.
• Linking with Infrastructure Managers to facilitate the removal of cameras above road decks areas during already programmed road closures, saving cost and traffic impacts.
• Relocating Camera’s causing access issues and/or injuries.
• Giving operators at Lift Bridges control over the camera’s locally, to give them better traffic coverage at drop gates and coverage of pedestrian accesses during lift operations.
• Some camera’s remaining in position until suitable works are undertaken that can be utilised for their safe removal.
Project Case Study
Project Case Study
Project Case Study

CAMERAS

• Camera location assessments were carried out at each location supported by a detailed Risk Assessment along with specific location requirements and a number of recommendations were made that include:
  • 74 Cameras (60%) were found to provide little or no Infrastructure Protection value or that provide traffic coverage only.
  • 48 Cameras (40%) were upgraded, relocated to increase coverage, improve access for maintenance and remove the use of EWP’s and equipment to reduce the exposure to safety hazards.
• Reduction on local staff travel times
Project Case Study

CAMERAS CONT.

• A new Asset Tagging and Mapping System to be able to identify individual cameras, their life cycle, location and servicing/maintenance details.

• The potential for a ‘whole of government approach’ with other government agencies provided with footage/analytics from the system such as:
  • Bridge Readings (Alignment Deviation, Load Limits, Power/Fire Boards)
  • Water/Flood Level Readings
  • Air Quality (Pollution, Bush Fires)
  • Road Traffic Incidents
  • Marine Traffic
Project Case Study

BENEFITS

• The use of analytics (camera and software warning systems) to reduce the workload on operators in the Control Room and dramatically increase the ability to detect potential risks to Infrastructure;

• Some limited access to other key RMS departments to monitor footage for maintenance, processes.

• Analytics capability to supplement fire & life safety systems.

• Better Bandwidth

• Reduced Storage
Project Case Study

BENEFITS CONT.

• Documentation supporting project requirements
• Consultation with Asset and Region Managers.
• Pricing per Unit
• Consolidating a number of fixed camera’s with dual PTZ / Thermal providing the same or enhanced Infrastructure Protection coverage (Dual IP)
• Prioritising and Categorising of Cameras to store the footage for either 28 Days, 7 Days, on No Recording at all
Kangaroo Lesson #4

You are not safe, anywhere

WARNING: This will give you nightmares
Questions