19th International Congress on Modelling and Simulation, Perth, Australia, 12–16 December 2011
http://mssanz.org.au/modsim2011

# Crisis simulation exercises of terrorist incidents in the Australian water industry

**Jamie Crowe [a], Dave Birkett [a,b] and Helena Mala-Jetmarova [b,c]**

[a] *Truscott Crisis Leaders, Wembley Downs, Western Australia 6019, Australia*
[b] *School of Science, Information Technology & Engineering, University of Ballarat, Mt Helen Campus, University Drive, Ballarat, Victoria 3353, Australia*
[c] *Grampians Wimmera Mallee Water (GWMWater), 11 McLachlan Street, Horsham, Victoria 3400, Australia*
*Email: jcrowe@crisisleaders.com*

**Abstract:** Australian water organisations currently rank within the nine sectors identified by the Federal Government under the category of Critical Infrastructure (CI), as designated by the Attorney General's Department. As such, water from a CI protection perspective is considered to be a vulnerable target for terrorism.

Major global terrorist incidents such as the attack in New York in 2001 coupled with the media interest and associated amplification have highlighted the need for organisations to protect water infrastructure from future attacks.

The Victorian Government is leading the path to terrorism risk reduction of CI by the introduction of an Act of Parliament *Terrorism (Community Protection) Act 2003*, assuring that risk mitigation is in place across the state. One requirement under this Act is to annually practice plans and procedures in the form of scripted Crisis Simulation Exercises (CSE).

These CSEs are to ensure that water organisations are more resilient to meet the challenge and maintain business continuity during any future terrorist incident. This includes the interactions and timings of available resources, logistics with appropriate personnel as required and to the appropriate level indicated in the plans. These CSEs can incorporate live actions, testing equipment and personnel within all organisational levels.

It is considered that CI organisations which adopt these strategies enhance business survival and continuity, producing a resilient entity prepared for and resistant to penetration by an organised terrorist group or radical cell.

This paper provides an overview of a simulation framework to ensure preparedness suitable for mitigation of risk of terrorism in relation to the Australian water industry.

**Keywords:** *Crisis Simulation Exercises (CSE*), *terrorism, Australian water industry*

## 1. INTRODUCTION

Desk top simulation exercises have been an effective tool of Victorian water organisations in testing and providing the necessary opportunities to manage under pressure in a simulated crisis environment. In these CSEs the outcomes are not real, but effectively illustrate the potential issues which could occur during a real crisis such as a terrorist incident. This activity also enables the organisation to change processes and procedures to encapsulate a more appropriate response to such incidents.

The process of a CSE consists of the following sequence:

- Understanding the drivers and legislation,
- Establishing the CSE objectives,
- Assessing the risk and vulnerability of the water organisation,
- Designing a CSE script,
- Developing a CSE structure using the Australasian Inter-Service Incident Management System (AIIMS) (AFAC, 2004),
- Establishing a counter player team,
- Operation and delivery of the CSE,
- A 'hot debrief' to ensure that the identified feedback can be documented and improvements implemented.

## 2. CRISIS SIMULATION EXERCISES

### 2.1. Drivers and Legislation

To understand the drivers is an important component in planning a CSE which also assists in preparation of the exercise strategy. Drivers can vary from being prescribed by legislation such as in Victoria being mandated under the *Terrorism (Community Protection) Act 2003* as an essential service provider. This is to test the organisational capacity from the boardroom to the 'coal face' in day to day operational tasks.

### 2.2. CSE Objectives

The exercise objectives can represent testing of systems, plans, procedures, personnel and equipment. This is dependent on the legislation, industry standards or reasons for conducting a CSE.

### 2.3. Risk and Vulnerability Assessment

Risk assessment and identification of vulnerabilities can be achieved by establishing overall risk from a broad organisational perspective applying an organisational risk framework (Standards Australia, 2004). This process can be used to analyse how this risk may occur to one or more water assets. When the vulnerability of an asset is identified, further investigation is then required to ensure that the CSE (i) can be achieved, and (ii) the CSE scenario is realistic and conceivable.

An example of an organisational risk framework is illustrated in Tables 1 to 3. Table 1 lists the consequence ratings for economic, environmental, social and reputation risks, which establish the potential impact and consequence to organisational image and operation. Table 2 represents the likelihood of the incident to be further applied to identify the overall inherent risk rating without any contingencies in place. Table 3 displays the overall risk using the total organisational risk framework. When mitigating actions are applied, the framework is referred to again in order to identify a residual risk rating.

Should a risk be identified as a high risk, the risk is then analysed further to evaluate how it could occur. The vulnerability of the asset or process is clearly defined and understood in detail, and each component of the risk is separated until it is possible to identify a 'point of failure.' This point of failure can then establish the feasibility of such an incident occurring to ensure the reality and credibility of the CSE.

Furthermore, the establishment of the organisational risk context includes the development of a framework for measuring, reporting and categorising risk. This framework should be relevant to the specific organisational responsibilities, be easily understood, and enable accurate and informative reporting and analysis. Within the context of terrorism, consideration of interdependent industries risk should be evaluated, such as power loss and transport failure.

**Table 1.** A Typical Organisational Risk Framework – Consequence Matrix.

| Risk Rating | Economic | Environmental | Social | Reputation |
|---|---|---|---|---|
| 5 | Cost to the organisation greater than $1 Million | Irreparable damage to the environment and the permanent loss of species or fauna | Single or multiple fatalities | Multiple stories and media both nationally and internationally |
| 4 | Cost to the organisation of $1 Million | Greater than 1 year to repair the damage, major litigation impact | Multiple hospitalisations of personnel or public, and/or multiple loss of permanent employment | State and national multiple stories in papers and media |
| 3 | Cost to the organisation $500,000 | 1 year to repair the damage, major litigation impact | Single hospitalisation of personnel or public, and/or a single loss of permanent employment | State and national media enquiries |
| 2 | Cost to the organisation $100,000 | 4 weeks to repair the damage, minor litigation impact | Major medical treatment required of personnel or public, and/or a temporary loss of permanent employment | Local and state media attention, multiple stories in papers |
| 1 | Cost to the organisation $10,000 | 1 week to repair the damage, no litigation impact | Minor medical treatment required for personnel or public, and/or no loss of permanent employment | Local media exposure |
| 0 | Cost to the organisation less than $10,000 | Nil damage to the environment | Nil medical or employment impact | Nil media enquiries |

**Table 2.** A Typical Organisational Risk Framework – Likelihood Matrix.

| Rating | Likelihood |
|---|---|
| 5 | Imminent |
| 4 | Possible within the next 12 months |
| 3 | Possible within 2 years |
| 2 | Possible within 5 years |
| 1 | Possible within 10 years |
| 0 | No risk foreseeable |

**Table 3.** A Typical Organisational Risk Framework – Overall Risk.

| | Consequence Rating | | | | |
|---|---|---|---|---|---|
| Likelihood | 1 | 2 | 3 | 4 | 5 |
| 1 | | Low | Medium | Medium | High |
| 2 | Low | Low | Medium | Medium | High |
| 3 | Low | Medium | Medium | High | High |
| 4 | Medium | Medium | High | High | High |
| 5 | Medium | Medium | High | High | High |

### 2.4. CSE Script Design

Design of the exercise script enables testing of capabilities in managing assessed risks which result from the overall risk analysis and extent of the vulnerabilities. The script can include single or multiple 'jeopardies,' when single or multiple incidents occur, respectively. Additional jeopardies or incidents are added to the CSE script to increase the pressure level of the CSE.

Each of the jeopardies should be spaced according to the experience and capability of the tested personnel. The initial jeopardy is the primary trigger for the CSE. Subsequently, the jeopardies are inserted to ensure that the CSE progresses with adequate pressure.

The CSE script also indicates the times, identities and sequence of events during the CSE. The timing of the CSE can provide some challenges which should be previously identified and potentially clarified. For example, most terrorist incidents rarely occur between the hours of 9 am – 5 pm from Monday to Friday, so consideration to run the CSE outside of the normal operating hours should be evaluated.

### 2.5. CSE Structure

In the Victorian water industry, a CSE structure is normally developed using the AIIMS framework. This system originates from the United States model and has been extensively adopted and utilised in Australia.

The structure is relatively simple and can be extrapolated as required for the various industry sectors. An example structure is provided in Figure 1. There are eight line functions reporting to the incident controller, providing a managed structure to cater for any crisis. Standard colour coding as indicated in the Figure 1 is used during the crisis to immediately identify the roles and functions of all personnel.

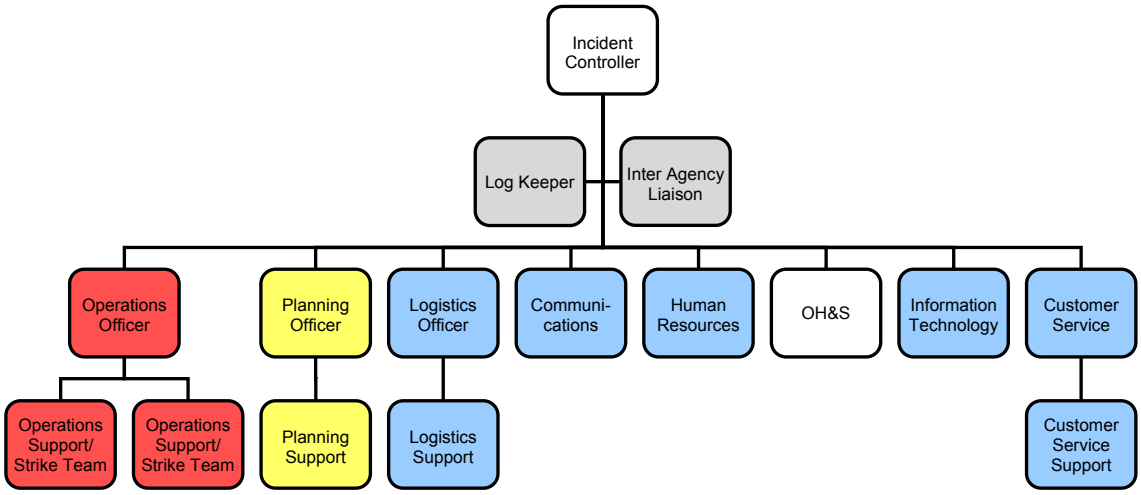


**Figure 1.** A Typical CSE Structure Using AIIMS.

### 2.6. Counter Players

The counter players are the 'engine' of the CSE as they feed pre-determined inputs using the assessed risks. The counter players act in various roles such as terrorists, government organisations, counsellors, police, media and others as required. Counter player roles may be undertaken by board directors, management or operational personnel from the organisation.

Selection of the counter players should comply with the following criteria:

- They are able to act their roles as if the terrorist incident was real,
- They are able to adhere to the CSE script as it is written to ensure all of the CSE objectives are achieved.

To become familiar with their roles, the counter players are provided a copy of the CSE script immediately prior to the exercise in order to understand their roles and exercise timeframe. The counter players also control the speed and intensity of the CSE under the direction of the exercise controller.

### 2.7. CSE Operation and Delivery

A real crisis may extend from a period of hours, weeks or months, whereas the CSE has a compressed timeframe to simulate pressure and stress levels of a real terrorist incident. Typically, the CSE may operate from 3 hours to 2 days depending on the exercise requirements (Birkett et al., 2011). In the Victorian water industry, most CSEs are scheduled for a 3 to 4 hour period.

The operational structure of the CSE consists of exercise management and control element, inclusive of an exercise active simulation element. The management and control element include the exercise manager, controller, assessors and observers. The active simulation element is represented by counter players, the Incident Management Team (IMT) and the Crisis Management Team (CMT). This structure is indicated in Figure 2.

A briefing is undertaken prior to the CSE for the counter players, IMT and CMT, where rules of the exercise are clearly communicated and understood. It is also important to highlight the timing of the exercise with the protocols used to start and end the exercise. A fall back protocol should always be highlighted if a 'real life' incident occurs.

The CSE, when initiated, operates at a frenetic pace with exercise inputs building the stress of a simulated terrorist incident. During this initial stage, it is crucial to activate the CSE primary trigger in order to initiate

the IMT to manage the response phase. As the crisis progresses, the initiation of the CMT is considered as a consequence of the levels of reputation, litigation and business continuity issues arising.

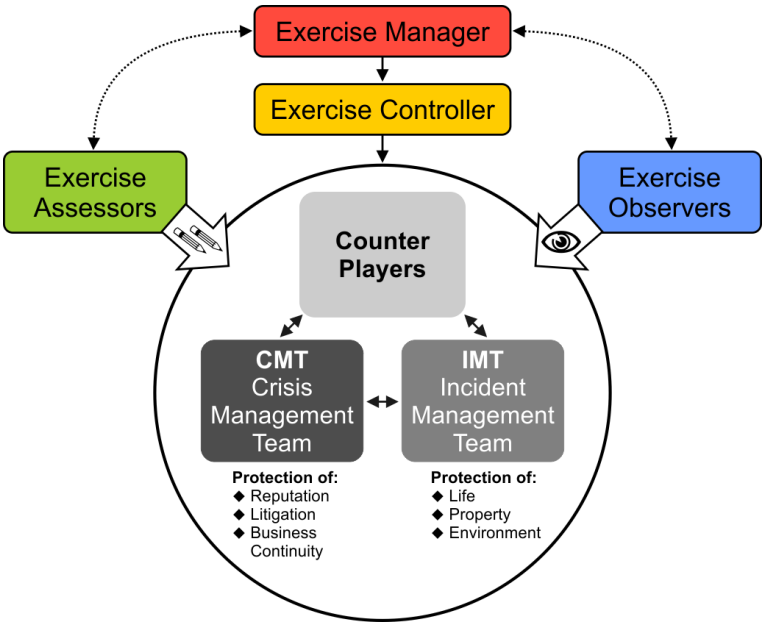


**Figure 2.** A Typical CSE Operation.

Fast response actions are required from the IMT and CMT to ensure minimal damage is experienced and the normal operations of the water organisation are restored. The organisational capacity to operate as 'business as usual' requires to be maintained to deliver the services and goods, which may be at risk in an incident.

Generally in the Victorian water industry, the exercise is delivered using three independent rooms, each for the counter players, IMT and CMT. The rooms should be located in close proximity to enable adequate communication and information transfer. These areas are also required to be easily accessible by exercise assessors and observers.

### 2.8. A Hot Debrief

Directly after the exercise completion, a hot debrief is required to capture the exercise outcomes. This is to ensure that the identified feedback both positive and negative can be documented, and relevant action plans implemented to correct vulnerabilities and issues identified during the CSE.

Under the topics of 'sustain, fix, improve,' all exercise participants are encouraged to openly contribute to highlight inefficiencies to ensure that the opportunities for future improvements are achieved. The results of the hot debrief are then documented in a written report highlighting actions and improvements necessary for the organisation.

## 3. SUMMARY

The paper introduces the CSEs as an effective tool to prepare the water organisations for any future terrorist incidents. The *Terrorism (Community Protection) Act 2003* in Victoria has assisted the CI organisations in implementing the CSEs, and understanding exercise requirements and objectives.

Prior to a CSE, the risk process is adopted to analyse and identify the vulnerability of the organisation. Subsequent design of the CSE script reflects the overall risk analysis and the extent of the vulnerabilities. To form the appropriate CSE structure, the AIIMS framework, which has been extensively adopted in Australia, is applied. In the Victorian water industry, operation of a CSE requires various designated functions such as exercise manager, controller, assessors and observers as a CSE management and control element, and the counter players, IMT and CMT as a CSE active simulation element. The CSE is normally concluded by a 'hot debrief' and a written report to assure that exercise outcomes are documented for future improvements.

## REFERENCES

AFAC (2004). Australasian Inter-Service Incident Management System, third edition. Australasian Fire Authority Council (AFAC), Melbourne, Australia.

Birkett, D., Truscott, J., Mala-Jetmarova, H., and Barton, A. (2011). Vulnerability of Water and Wastewater Infrastructure and its Protection from Acts of Terrorism: A Business Perspective. In: *Handbook of Water and Wastewater Systems Protection, Series Protecting Critical Infrastructures,* Clark, Robert M., Hakim, Simon, Ostfeld, Avi, eds., Springer, USA.

Standards Australia (2004). AS/NZS ISO 31000:2009 Risk Management - Principles and Guidelines, third edition 2004. Standards Australia, Sydney, NSW and Standards New Zealand, Wellington.