

2006 Mass Transport Security Conference

Panel Discussion : Gaps and Trends in Operational Protocols and Response

Presenter: Paul Murphy, Manager Security Consulting, GHD
Date: 5 December 2006

Introduction and Background

Operational Protocols and Response – General Comments and Observations from Overseas

- Security is not an add-on to the transport systems operations. Security is an integral part of the operations and needs to be embedded into customer service, network operations, infrastructure design and safety
- Management of security, safety and systems are not instinctive behaviours – they are learned behaviours – learned in training and learned in action.
- Having control over your employees – particularly those directly responsible for safety and security was considered by many transit authorities as a key to providing improved security and operational capability / resilience – due to the continuity of training, shared ownership and participation, and understanding of 'normal behaviours of the system (i.e. easier to identify unusual activities)

Operational Protocols and Response – General Comments and Observations from Overseas (2)

- Many international transit authorities have their own transit authority police with full policing powers over all transit system operations – including first response capabilities and specialist teams (canine units, search and rescue) – work very closely with local jurisdictional police to supplement resources
- Most overseas transit systems have control over the network, including infrastructure, tracks, vessels etc and operations – a different model to many Australian systems where ownership may be distributed
- Problems generally occur at interfaces – between networks, between buildings, between people.....
- International experience shows that organisations exposed to real events or near misses are better able to deal with the 21st century security environment

Responses to Managing Hoaxes and Catastrophic Incidents

- What is a Hoax? Do you treat hoaxes differently to real events?
- Determining whether you are dealing with a 'live event' or a hoax – can you tell the difference initially?
- What is a "highly regrettable incident" for your organisation?
- How do you respond to a threat?
- Who within your organisation is capable and authorised to make a decision regarding these issues – remembering that a decision may save lives or be highly regrettable?

Responses to Managing Hoaxes and Catastrophic Incidents

- Threat (mail, phone, email, letter)
- Suspicious package or substance
- Suspicious event
- Suspicious symptoms
- Multiple symptoms at single location
- Multiple symptoms at multiple locations
- Suspicious / actual event confirmed at a secondary or tertiary location in the community
- Progressive increase in credibility

Responses to Managing Hoaxes and Catastrophic Incidents

- Deal with each as a potential incident
- Manage hoaxes as if they were a real incident
- Remember hoaxes have the potential to cause as much damage as a real event
- Hoax events have the potential to deplete limited community resource and first response capability. In major US transit systems where transit police are employed a IED, CBRN threat can only be reported as a threat by a trained and capable first responder
- Other staff are trained to only cordon and observe.

Response to the Detection of Explosives on Passengers

- Much of the current research has the aviation industry as its focus.
- The terrorist attacks in Madrid and London highlight that mass passenger surface transport is a key target. These modes include bus, rail and ferry.
- What do you do if you discover someone has an explosive precursor during some form of ETD testing?
 - ⇒ Particularly when it is more than simply residue and they are determined to carry out their goal?
 - ⇒ Are our response procedures sufficient to deal with these threats?
 - ⇒ Are our screening arrangements sufficient and effectively designed for this change in thinking?

Trends in Security

- Integration of security, customer services and network operations
- Heavy focus on security technology by some transit systems – firstly you need to understand why you are using technology and what it is going to do for you
 - ⇒ Most of the technologies work, but their effectiveness in an operational environment is questionable
 - ⇒ Don't always believe the technology sales people
- Heavy focus internationally on resilience and consequence management
 - ⇒ If we can't prevent (given that most transit system operators do not have the ability to capture potential terrorists) what do we do?
 - ⇒ We can limit the exposure – through reduction in vulnerabilities (make more difficult and transfer / displace the threat)
 - ⇒ We can minimise the consequences

Questions?

Paul Murphy
Manager Security Consulting, GHD Pty Ltd

+61 2 6245 1946
paul.murphy@ghd.com.au

