

Live on the Edge or Make your own Edge

Aviation and Crisis Leadership

By

Jim Truscott & Robert Kilsby

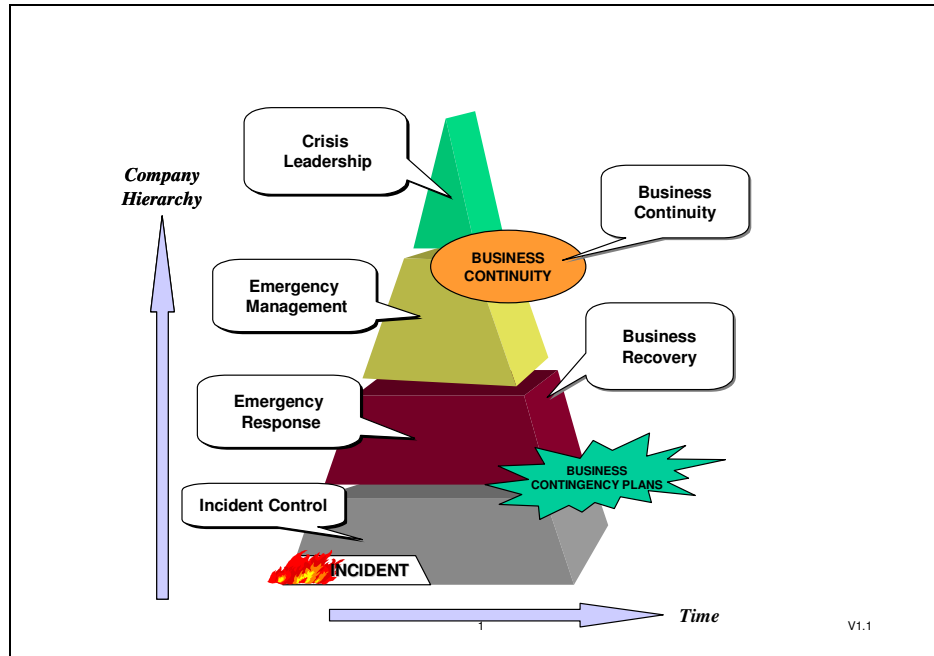
What if the main air traffic control centre at one of Australia' international airports lost its power? Even if the blackout only occurred for 12 minutes, would this have been enough time to lose radio and radar contact with 20 planes in transit? What would you say if the power was restored after only two minutes, but it took ten minutes for the system to be rebooted? This sequence of events allegedly occurred at Sydney in July 2000. We now have sky marshals patrolling the skies, but are they enough, and would ground marshals have prevented this business outage if it had been an act of terrorism?

Now imagine this. What if a bunch of seaborne suicide terrorists sped out onto the runway on motorbikes and literally blew themselves up against ten aircraft on various parts of the airport? Every time we land on the Botany Bay runway we think about these sorts of sequences. With a background in counter-terrorism, special operations, underground warfare and commercial crisis management, one's mind often works through these Red Cell sequences and eventualities. Incredulous and borderline as it maybe to some, this is precisely what the Tamil Tigers did to an airbase in Sri Lanka a few years ago with satchel explosive charges strapped to their chests. Why can't it happen here, in a democracy? The exposed seaward runway is a wide open to a high-speed direct assault, as indeed is some bush and riverine approaches to all other capital city airports in Australia.

What if only twenty percent of these events were true, but it happened at three major eastern states airports simultaneously? Think about it. Whether you do or don't, other people certainly are. People such as recently captured al-Qaeda operations chief Khalid Shaikh Mohammed spend their waking time planning the destruction of our western infrastructure and societies. So how much security is enough? The reality is that the ever hardening concentric rings of physical, information and personnel security, properly executed, will go a long way to successfully deter, expose and prevent the foreseen rational attacks and the unforeseen irrational attacks alike. Under this model of fused safety and security, layers of toughness are the only way of dealing with terrorist's preferred method of delivery through suicide trucks, boats and planes. It is not inconceivable that al-Qaeda will use smaller planes to hit larger planes in the sky in the future, so the focus now has to be on all planes and not just big planes.

However think of this. What if Osama bin Ladin merely announced that due to Australia's support for the US, our national airline was a priority target along with the aircrew and their passengers. How many maintenance workers would turn up for shift? What percentage of aircrew would consistently volunteer for flight duty? Who among prospective passengers would continue to choose the airline? Would you? How would the share market react? The \$2.40 bill to leak the videotape and produce such paralysis is a small business cost for such business loss. Most companies will have an Emergency Response plan, which will be good enough to manage the consequences when fuel tankers are used as mobile incendiary bombs, but probably not efficient or directed enough to manage the traumatic emotional and commercial impacts from say, having lost complete aircrews when whole floors are taken out in

nearby crew accommodation hotels. Pilots, hotels, short-haul cabin crew bases, engineering services, tourist locations and navigation aids are all vulnerable to crises now and for evermore. This widening style of commercial crisis is not so much requiring of reactive management of say, a tattered reputation from cracks in wings, but it will demand the best practice of crisis leadership, to take the aviation sector and associated companies through the crises and beyond.



While the aviation sector is slowly adopting a formalized and long overdue approach to Safety Management Systems, now in these post S11 and O12 times there is an equal imperative to mesh security methodology to business integrity. All airlines and airports must look at their own assets as a saboteur does when they are analysing a target within a target system. When looked at through the eyes of the adversary, the threat can become a little clearer with critical people and infrastructure obvious. Here corporations and individuals need to think about threats in terms of intent and capability, and not with the traditional likelihood and consequence approach to managing risks.

The assessment of such acts is complex, and the aviation sector is not used to low-probability events such as suicide terrorism. In addition to formulae to support operational hazard management, there is need for similar formulae to give an answer to outrage risk assessments of potential security disasters. Most companies are familiar with overt assessments of consequence and likelihood. However, with security issues one needs to look at threat a little differently as the threat of an event is different to the potential of an event. When looking at terrorist threats, assessors need to think in terms of the terrorist's intent and capability. Intent in turn requires an assessment of both the terrorist's desire and expectation, while capability is a combination of the terrorist's resources and knowledge. The combination of capability and intent is expressed as high, medium, low or insignificant as shown in this matrix.

Intent	Capability			
	Nil	Limited	Significant	Comprehensive
Stated or known	L	M	H	H
General or suspected	L	L/M	M	H
None suspected	I	L	L/M	M
None confirmed	I	I	L	L

It can be difficult to assess intent and capability when the terrorist functions from underground cells and is unpredictable at best. This restriction limits assessor to look at the vulnerability of assets in isolation. However this is what a saboteur does when they are analysing a target within a target system. Suicide terrorists will use something like the CARVER acronym, and the aviation sector will find this acronym useful in assessing threats to assets within their responsibility, particularly if they do not have access to classified reporting. When looked at through the eyes of the adversary, the threat can become a little clearer, and in determining how much security is enough, a CARVER assessment can be used to look at the aviation operation from a terrorist viewpoint.

- **C** is criticality or relative importance. What part of your operation is most critical? For example a terrorist may seek to destroy the fuel farm in addition to concentrations of people to achieve maximum outage.
- **A** is for accessibility or ease of access. Smuggling a bomb onto an aircraft is not as hard as placing one in the passenger terminal or sniping at an aircraft; so easy access targets are often preferred.
- **R** is recoverability and how easily the asset can be repaired, replaced or brought back on line. This downtime thinking may indicate a further threat to repair and spare parts facilities, as a terrorist will seek maximum bang for buck.
- **V** is for vulnerability and the ease with which people and infrastructure can be put out of action with a hammer or a spanner. Martyrs are just as scared as anyone else when it comes to delivering the final blow, even with the motivation of 70 virgins and a place in heaven. All terrorists will look for the easier way. For example, the Bali bombing is alleged to have only costed the terrorist's about \$30,000.
- **E** is for effect. Terrorists will concentrate on targets that will cause the greatest adverse effect on the population, such as could be caused by a disruption to multiple airports or lead to the failure of a national airline. Suicide terrorists favour spectacular attacks that have high symbolic value, cause mass casualties, and severe damage to the economy. In the face of security risks, airline companies need to act as an anti-access and anti-denial team regardless of international or regional competition.
- **R** is for recognition and answering the what is it, and the what, where type questions? It is the ability to actually to identify one target from another. The effect of their action will be minimised and even counter-productive to the terrorist planners' objective if the wrong target is hit, but note that not all local terrorists are as smart as Osama bin Ladin, and some attacks may not be logical.

	Terrorist Thinking	Aviation Thinking
Criticality?	Is it a high-value target?	What are my critical systems?
Accessibility?	Is it easy to reach?	How effective are my layered security measures?
Recoverability?	How long will the outage or outage last?	Do I know how quickly my systems can be restored? Do I know how quickly supplier's systems can be restored?
Vulnerability?	How easy is it for me to destroy?	Do I know the critical components of my business, and what are their security barriers? What are the critical supporting components to my operations?
Effect on the local population?	Will the psychological effect achieve my aim?	What is likely to generate public pressure? What current public attitudes can be compounded?
Recognizable?	What does it look like, and where is it?	Can simple recognition be prevented in some harmless way?

Then apply and practice the ultimate insurance for business continuity, corporate reputation, and liability issues...crisis leadership. Think the unthinkable when it comes to suicide terrorism and use these scenarios to identify risks and test business continuity plans. Scenarios are traceable paths into the uncertain future forming the foundation to allow crisis leadership to take the corporation beyond bin Laden, back to opportunity and competitive prosperity; back to the future. Indeed, anything less is tantamount to sending aircraft on their journeys with imprecise navigation coordinates and insufficient fuel to reach any reasonable destination. Total security is a great challenge.

TRUSCOTT TRUSCOTT is a niche consultancy focused on preparing executives and managers for the
Crisis Leaders unthinkable but, unfortunately, the inevitable.

We consult to organisations large and small throughout Australasia and Asia. We have assisted hundreds of clients in government, multi-national, medium, and small organisations. We have wide experience in the resources, energy, and finance sectors.

Jim Truscott, the founding director of TRUSCOTT, spent 25 years as a strategic group manager and leader of operational teams in high-risk international engagements planning and controlling politically sensitive government operations for the successful resolution of regional and international crises. Drawing on that wide experience, he now consults to industry and government on crisis leadership and on risk and emergency management.

Robert Kilsby is skilled in controlling crises from 20 years in the SAS in totally hostile and confusing situations and now on the second battlefield as a crisis leadership practitioner.

Contact TRUSCOTT at jtruscott@crisisleaders.com or visit www.crisisleaders.com