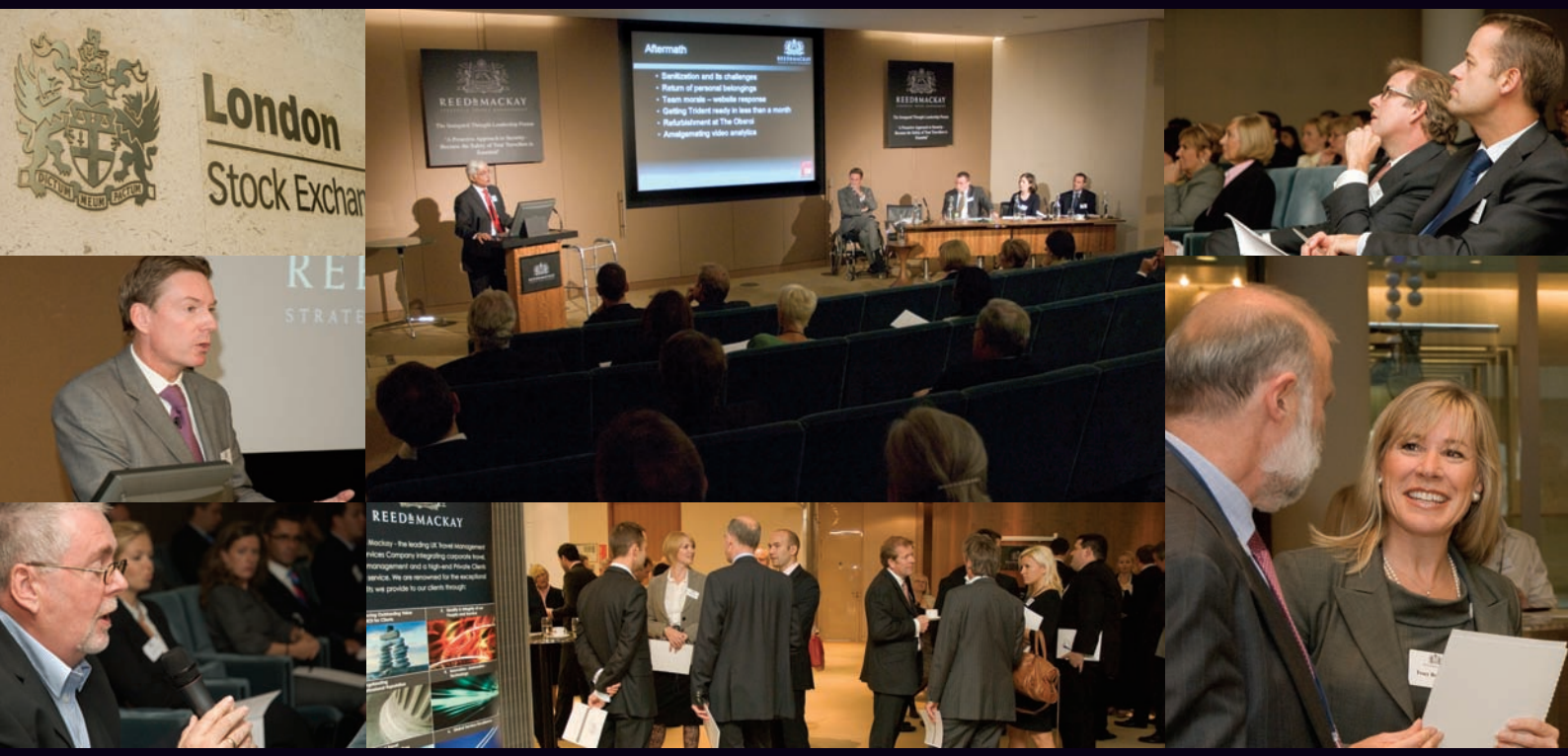
THOUGHT LEADERSHIP FORUM

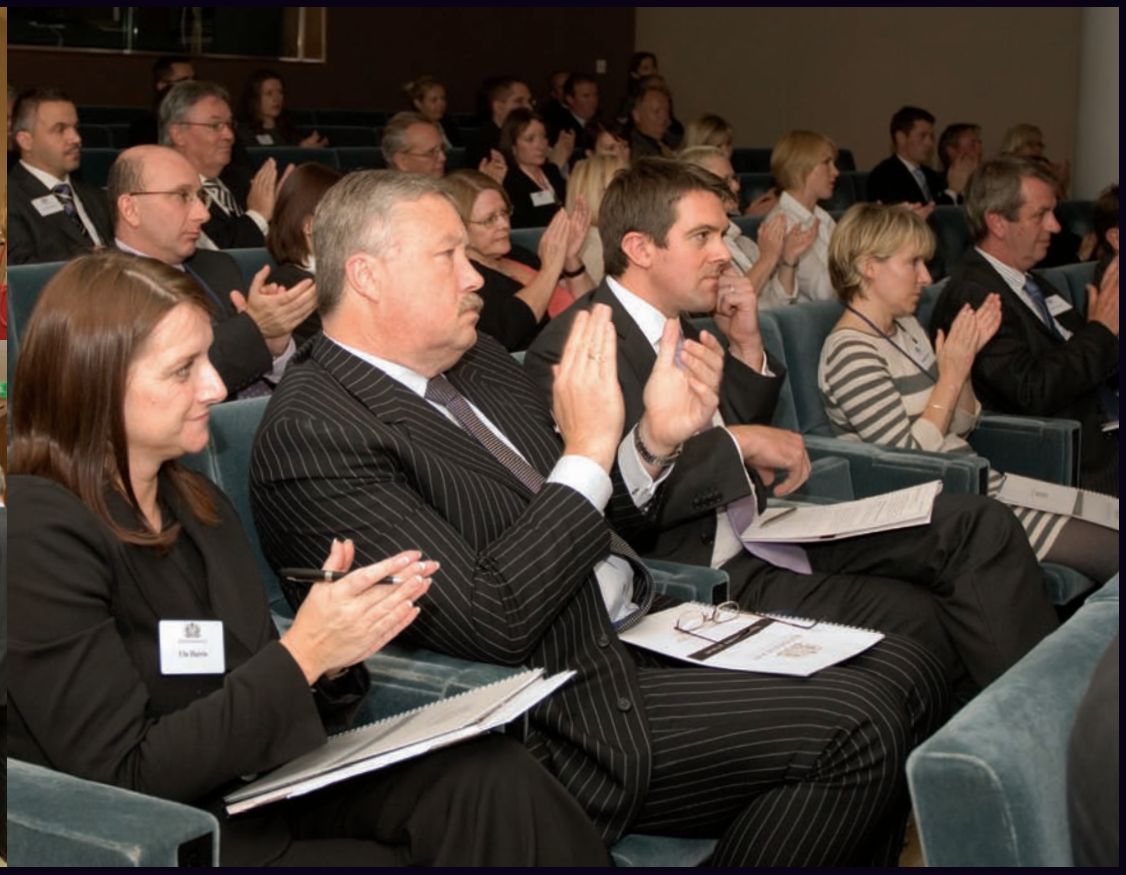
A Proactive Approach to Security -
Because the Safety of Your Travellers is Essential

Venue: The London Stock Exchange
Date: 1st October 2009



Qualitative Report

REED&MACKAY
STRATEGIC TRAVEL MANAGEMENT



Inaugural Thought Leadership Forum

A Proactive Approach to Security-

Because the Safety of Your Travellers is Essential

Reed & Mackay Travel's inaugural Thought Leadership Forum was held at The London Stock Exchange on October 1st. Over the previous six months qualitative research amongst our clients was commissioned to determine which issues were at the forefront of their minds.

As a result, this first debate focused on Security and Traveller Safety. A specialist and informed panel led by the BBC's Security Correspondent, Frank Gardner were brought together to explore how the landscape has changed and what it means for the industry and travellers' welfare in today's volatile climate.

The format for the debate was individual presentations, followed by audience Q&A with a chance for further conversation and networking over drinks later. The following qualitative report is based on extracts from those presentations and questions from an audience of 80 Reed & Mackay clients.

A Background to the Current State of Security

Frank Gardner has an OBE for his services to journalism and the scars to prove it. In 2004 he was shot six times at close range by Al-Qaeda gunmen while filming in Riyadh, Saudi Arabia, but survived with major injuries. His insightful opening remarks set the scene for an interesting and lively debate.

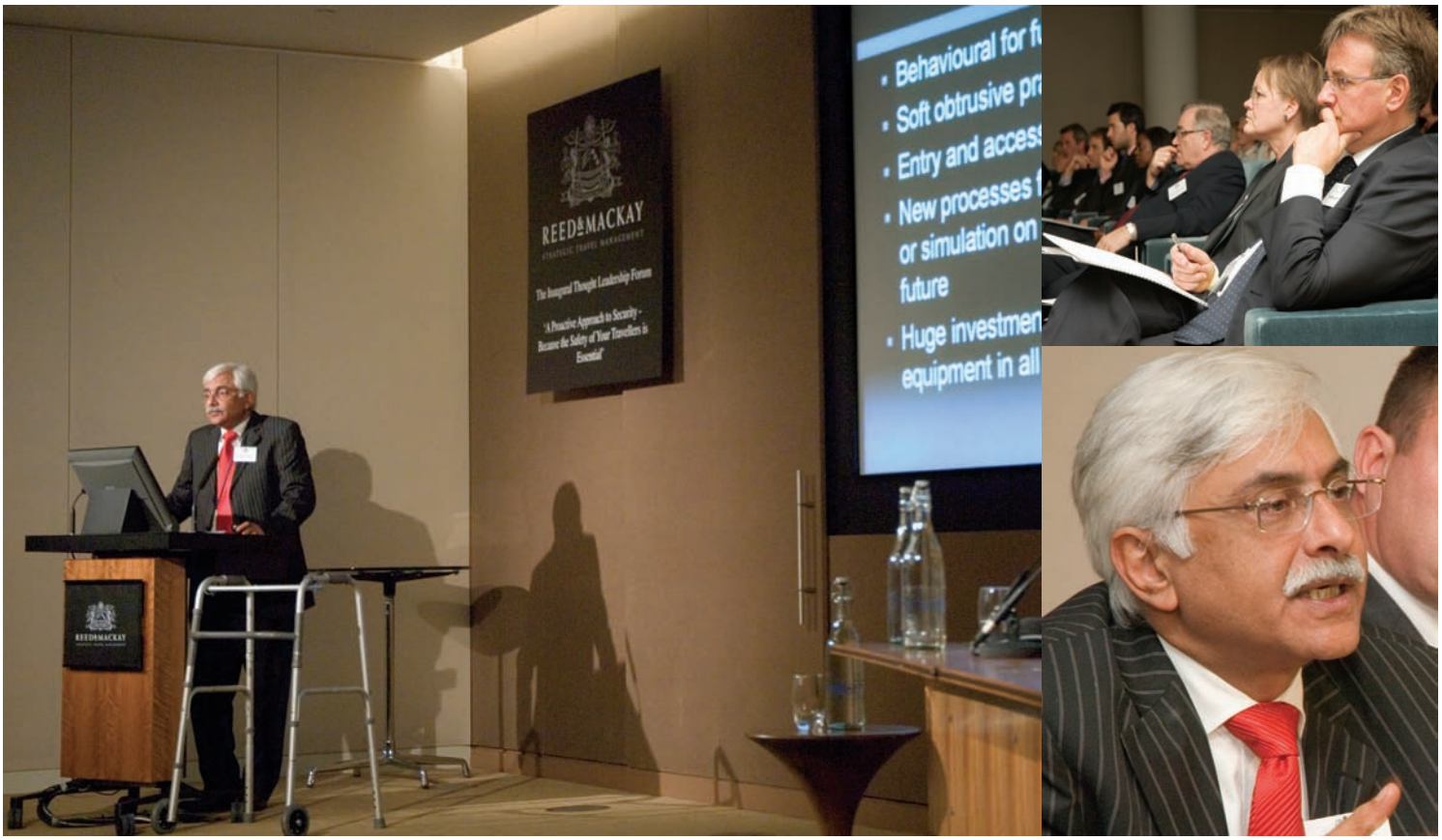
At present in the UK we are at a "Substantial" level of threat. This is based on the official public system of threat levels where 1 is set at "**Critical**", 2 "**Severe**", 3 "**Substantial**", 4 "**Moderate**" and 5 "**Low**". The present level is down from levels 1 and then 2, set after the 7/7 bombings.

Things seem to be getting better then? Gardner is a journalist and sees the bigger picture. To prove it he screened his news report shown on the BBC, Friday 25th September, (less than a week before this conference). The story concerned a 24-year-old Saudi member of Al-Qaeda who gave himself up and was flown to meet Saudi Prince Mohammed bin Nayef in Jeddah. Seemingly a small victory in the battle for hearts-and-minds in that region. Except this wasn't.

> "The point is that the security threat is evolving. New methods require new strategies"

The man had carried a bomb inside his body for 30 hours, unseen by metal detectors, and detonated it using a mobile phone whilst standing next to the prince. The first case of a Body Bomb. The Prince survived only because the terrorist's body absorbed the bomb-blast. A member of the audience later asked if the event really happened, so unbelievable sounding was the story. Shots from Saudi TV are on YouTube for doubters. And who thought planes would hit the Twin Towers?

The point is that the security threat is evolving. The threat also comes from some unsophisticated directions, not just complex plots. These should be given equal importance and not be forgotten. The experts of old, with knowledge of, say, the IRA, are almost redundant. New methods require new strategies.



Caught at the Sharp End

Following on from Gardner's timely reminder was Mr Rattan Keswani, President of the Trident Group of Hotels including The Oberoi, Mumbai. Keswani had flown from India especially to attend the conference.

In November 2008 ten gunmen from the Lashkar-e-Taiba extremist group armed with AK47's and grenades, took over a boat and crossed from Pakistan. They launched a commando style raid, separated into twos and entered properties across the city of Mumbai including the Oberoi and Trident hotels murdering 163 innocent bystanders and hotel guests, and Keswani was there. His first-hand account covered the day itself, how his hotel group and staff dealt with the aftermath, the implications, the consequences and what steps they have taken for the future.

> "The UK security firm suggested the only thing not covered in the manual was an amphibious attack by commandos"

Keswani's prelude reiterated the fact that the global security threat is evolving. In the 19 months before the events of 26th November 2008 his hotel chain had been working on a security manual. The main threats were seen as: **fire; bomb; intrusion**.

The manual covered everything from how to handle the media, practice drills, intelligence and how to keep running a day-to-day business without intrusive security. So thorough was the manual, the UK security firm advising suggested the only thing not covered was "an amphibious attack by commandos"!

India has a government alert of some kind about every 14 days and people have become immune to them. This, combined with the unexpected nature of the attack, allowed the terrorists a free hand. They entered a number of buildings across the city, murdering and taking hostage innocent bystanders and hotel guests. The attacks were brazen and a step-up from the norm. Terrorist groups including Al-Qaeda seem to operate "aspirational" terrorism, designed to shock in its audacity.

Although 163 people were killed, the hotels' disaster recovery manual worked in that everyone who could

be was evacuated safely. The problems were many and largely unforeseen though. Most security systems look at a constrained location, not multiple locations.

Despite evacuation, people scattered through many exits with no designated "safe" place to go. Knowing who was safe was impossible. Added to this there was no trauma centre or evacuation coordination from Government bodies. Confusion reigned and although the Chief of Police was there, no central control was established. Responsibility was passed from the Police to Naval Command to National Security Guards. Crowds gathered outside to watch proceedings, endangering themselves and getting in the way of security forces. The army requested sprinkler systems be switched off - fire tends to smoke out terrorists but some rooms still had guests in. The guests were stuck in their rooms not knowing what to do. This problem was exacerbated by mobile phone calls giving them "news" that was at best vague and at worst terrifying. A media siege ensued and the hotels were quickly blamed for lack of answers.

When do you give the all clear? How do you protect valuables once you've told guests to leave them behind? How do you build team morale? How do you rebuild, literally, the business?

The initial aftermath threw up many issues. When do you give the all clear? How do you protect valuables once you've told guests to leave them behind? How do you build team morale? How do you rebuild, literally, the business?

From here flowed a list of things-to-do and lessons learned:

Video analytics. CCTV and a separate crisis centre in another city, for example Delhi, which can help co-ordinate events.

Behavioural training. Training staff to become more aware of unusual behaviour. This point was underlined by the recent attacks in Jakarta where the terrorists were actual guests in the hotel.

Entry and Access. Use unobtrusive surveillance along with bollards, scanners, boom barriers or metal detectors. We need to balance these outward signs of security with the need to keep the ambiance of a luxury hotel.

Investment. Huge investment needed for training theory, practice and new drills for similar attacks or simulations of possible future attacks. Similarly, investment for new equipment in hotels is crucial. The question to constantly ask; "is it necessary and is it enough?"

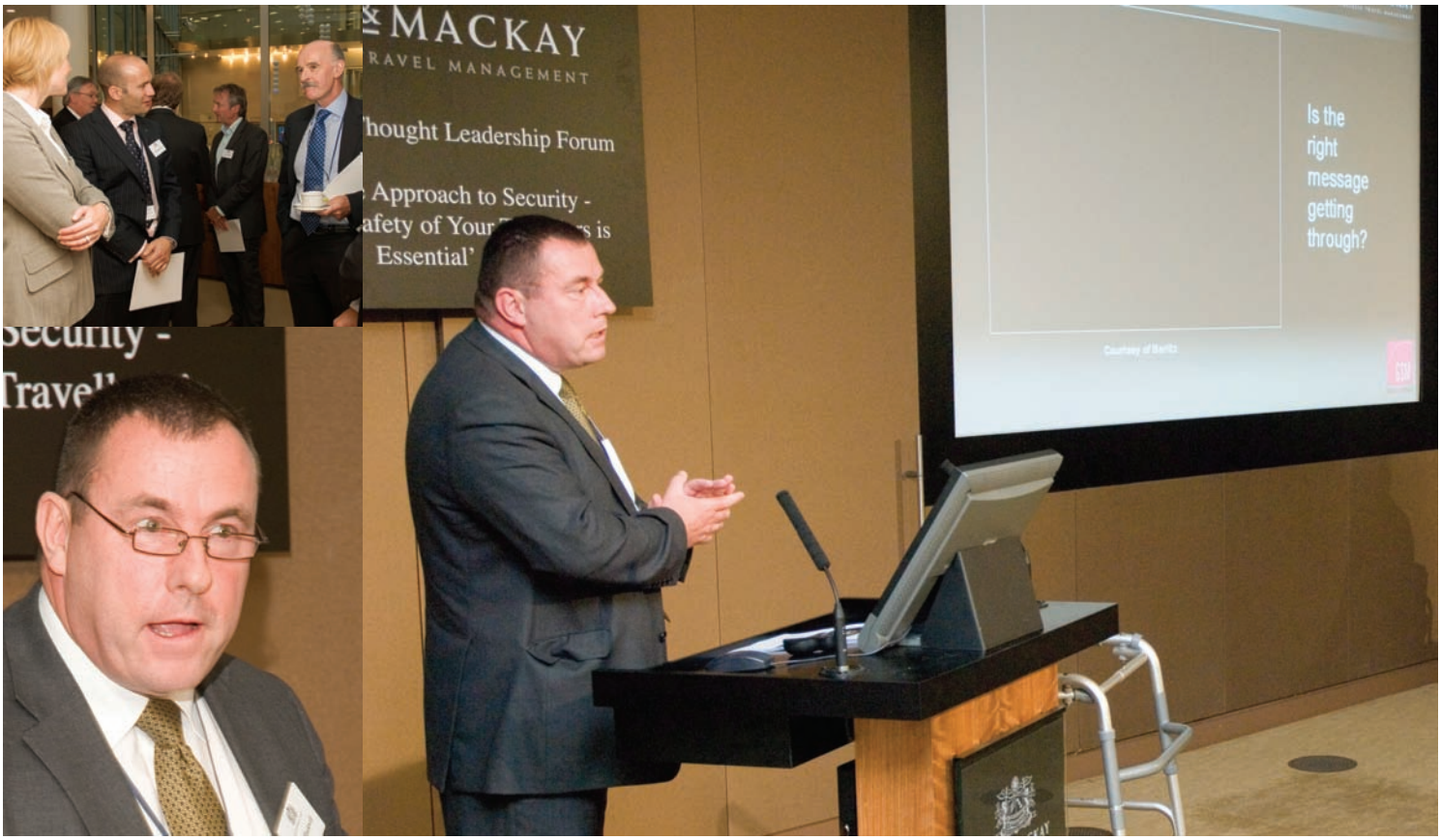
Cooperation. There's no real way you can do things on your own. A trained private security force can only do so much, so you need to work with the civic world.

Challenges. Agencies and auditors will overwhelm you with ideas but nobody is willing to take ownership and run it for you. They will provide lots of ideas; show you where the faults were and what you could do better. Ask them to 'set up shop' and run it for you and no one will take it on. The media generally are not useful. There is also a lack of uniform legal and insurance frameworks that run across countries. Security advisers for different companies have varied requirements. Surveillance and intelligence needs to be better coordinated.

Future prospects.

Keswani ended by stating future terrorism may not be the version we see today. Any building in any city could be a target, not just in the Middle East or South East Asia. It could be a similar attack or new versions with gas, viruses or worse. And attacks will happen. Fanatics have a death wish and will breach some layer of security. Racial discrimination, social barriers, lack of education, religious fanaticism, and inequalities in the basic quality of life will all play a part. If the world does not become more equitable we will see new challenges.

Keswani was the only civilian on the day allowed into the hotel by troops. The Oberoi had been his home for 4 years and for him it was a family thing. He said he felt helpless as he saw the bodies of people, some of whom he'd known for many many years. He says he is Indian enough to be fatalistic; "If it happens, it happens". When asked if the terrorists could be stopped if they ever came back, he said it wouldn't be easy for them. The intelligence is better now, and trained forces help, but you'll never stop a determined attack at every level.



Creating a Safety and Security Policy

Having heard about the reality of a terrorist attack, Andy Blackwell spoke about what to do in practice. Blackwell is Head of Aviation Security at Virgin Atlantic and has overall responsibility for the management of the airline's global aviation security programme and emergency procedures. His duties include threat assessment, emergency response, and providing senior executives with high-quality intelligence and strategic direction to ensure business operations remain secure, resilient and compliant.

Blackwell's approach to the subject is direct and he manages to find black-and-white amongst the shades of grey. He observed that before 9/11, security was usually 'AOB'. Now it's top of the agenda.

Collaboration and consultation is key to a successful security policy. Human factors affect protocol and the "big stick" approach rarely works. Indeed, it "de-motivates" people. A more proactive approach will create resilience and buy-in.

Security needs to be seen as non-negotiable and all-inclusive, from top down and bottom up. It's not an add-on. Everyone is responsible for safety and security, not just the experts. If everybody lives it then it becomes a potent force. Forewarned is forearmed and the more you know then the better equipped you are.

> "The trick is to keep things simple. Make compliance attractive by stripping it back and making it easy to incorporate into daily routines"

Official regulation will influence a company's policy but you should exceed the mandated standard, especially if risk assessment indicates it is prudent to do so. The trick is to keep things simple. Make compliance attractive by stripping it back and making it easy to incorporate into daily routines. Flexibility should be built in too, making it "future-proofed" and easy to adapt.

Different factors can influence the creation of a policy. Duty of care to staff and customers is paramount. Keeping risks low is important but not always easy. A simple formula illustrated this: Good and Fast doesn't mean Cheap. Any two positives from this formula will always make a negative. Safety can be used as a marketing tool though. For example, Virgin has won custom from competitors because of their security standards. Legal implications can arise. How good was your risk assessment? Will your decisions stand up to scrutiny or the coroner? Not only that, your reputation might be at stake - all bad for business.

"A simple formula: **Good** and **Fast** doesn't mean **Cheap.** Any 2 positives from this formula equals a negative"

Once you have a policy how do you keep it fit for purpose? Ensure the policy is communicated and understood. Keep it fresh. Regular reviews will help stop complacency. Forward-looking intelligence should be utilised as much as possible. Training and efficient technology will help you anticipate and "plan for the perfectly probable".

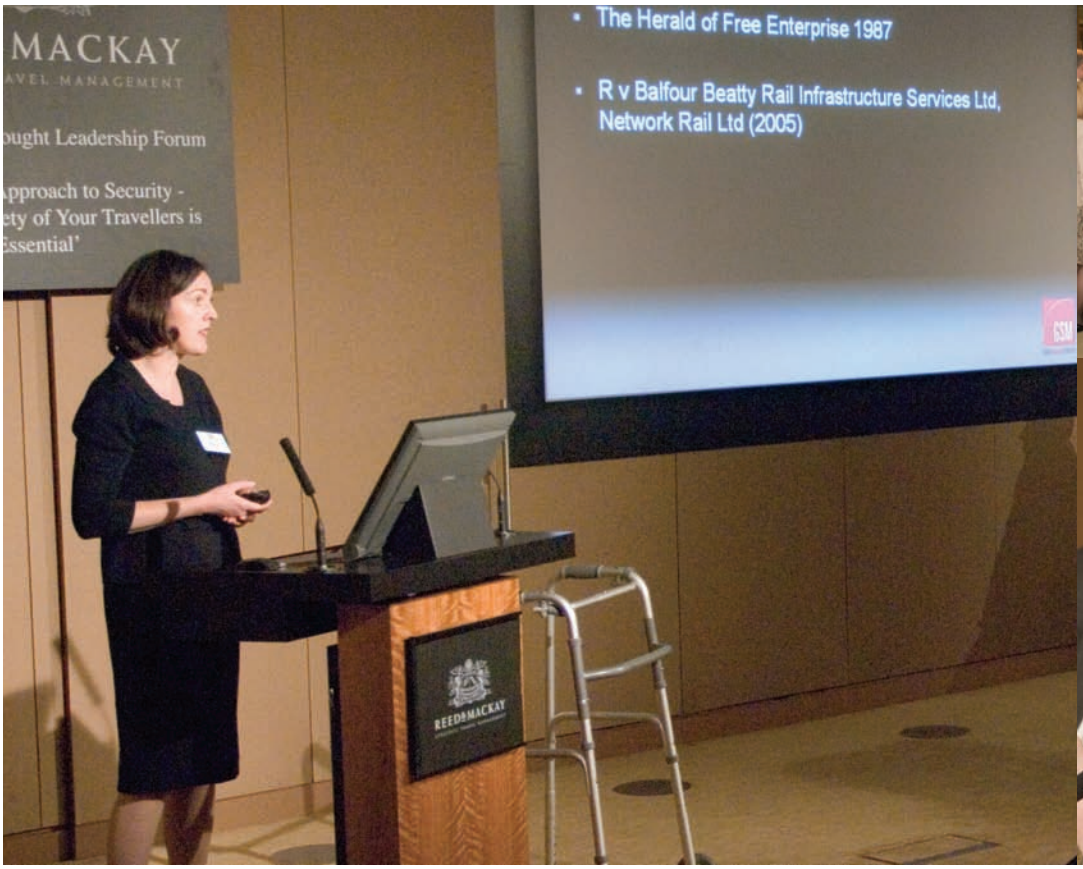
Security "good news" isn't sexy enough for the media. Blackwell gave the example of the intruder who scaled the fence at Heathrow a few years ago. He was quickly stopped, which was a success from Blackwell's stand-point, but the media saw it as a failure. It's not about selling newspapers. No news is good news.

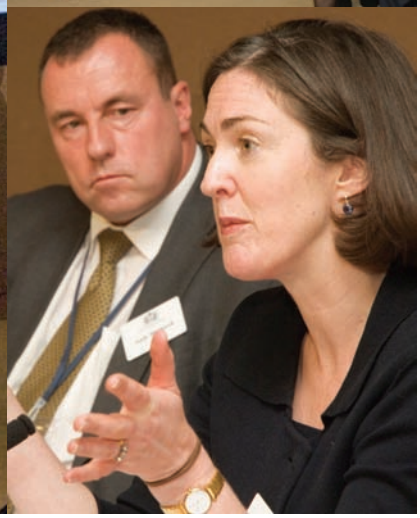
Best practices to help a policy work must include a range of options. Use in-house and industry forums to spread the word and help understanding. Use local security representatives, like a Neighbourhood Watch scheme, who know the lie of the land. Engage trusted partners, such as other airlines – they're going through the same things as you. The CPNI (Centre for the Protection for National Infrastructure) website has a Security Culture Toolkit which looks at issues affecting the business e.g. do you want your hotel to be a fortress? Sign up for MATRA, the Multi-Agency Threat and Risk Assessment body. It's not just governments interested in this issue. You need to get industry, the police, immigration, customs and excise, foreign office and others to sit round the table. Everybody is a stakeholder and has something to add to the equation.

Security "good news" isn't sexy enough for the media. It's not about selling newspapers. No news is good news

What advice does the Department of Transport give the industry?
Well, how do we stop a bomb? One threat might be contained, such as liquids, but that creates another problem: larger crowds at airports. Again, the threat is evolving. Al-Qaeda have a fascination, an obsession using planes as weapons and aren't about to go away.

We should focus on the good though and maintain confidence and morale. Errors are part of life but we can reduce recklessness. A measure of success is the ability to advise, not criticize. **Communication is the key.**





Corporate Manslaughter & Corporate Homicide Act

Expanding on Blackwell's point that your decisions and risk assessment have to stand up to scrutiny, Fiona Gill explained the new Corporate Manslaughter and Corporate Homicide Act. Gill is a Partner at international law firm Davies Arnold Cooper where she heads the Health and Safety group. She advises companies and individuals on safety, health and environmental law.

Why do companies need a security policy? As an employer you have a "duty of care" to your employees and clients. So far, so normal, but the world's changed. Before the new law came on the books in April 2008 the only way to prosecute a firm was through the 1974 Health and Safety Act. There is now a wider trend for corporate prosecution, which has grown since events like the Herald of Free Enterprise disaster in 1987. At the time, P&O Ferries were the first company ever to be charged with manslaughter under the old act. The failure to bring a conviction, and the subsequent political and public pressure, helped bring about the new Corporate Manslaughter Act.

"There is now a wider trend for corporate prosecution, which has grown since events like the Herald of Free Enterprise in 1987"

It is now easier to prosecute an organization and senior staff. Only the most serious cases are considered that involve a failure in "duty of care". The "identification principle" has been established whereby names have to be proven.

In essence the law says:
"An organisation… is guilty of an offence (of corporate manslaughter) if the way in which the organisation's activities are managed or organised -

- causes a person's death
- amounts to a gross breach of the organisation's relevant duty of care to the deceased"

In law there is "real" risk and "everyday life" risk. Slipping on a staircase and cracking your head open is an unfortunate accident. Sending an employee into a terrorist hot-spot, however, carries a serious threat.

Risk assessment is now crucial. Companies need to put policies in place and review them regularly. If you don't do it properly and someone dies on your watch then the paper trail goes back to your initial policy. Your risk assessment is your first line of defence. And, don't shoot the messenger, it's not an option: you have to have one now, by law. Where companies can fall down is by not making their policies relevant. Your policy needs to be fit for purpose and implemented coherently with regular reviews. High standards cost money but without them you can be in trouble.

"Where companies fall down is by not making their policies relevant. Your policy needs to be fit for purpose and implemented coherently"

When Gill was asked how Partners in law firms make a decision based on the new law, she replied; "We're waiting to see as more cases come up". Apart from the refreshing honesty, a sign that this is still new territory.

Delivering Smart Messages with Smart Tools

So, you have your security policy. How do you make sure it works in the field? Matthew Judge brought some practical nuts-and-bolts advice to achieving security and safety with the smartest tools. Judge is Group Director for the Anvil Group, specialists in providing "Crisis Avoidance Services" for global and multinational corporations. The Anvil Group also runs the Employee Travel Monitoring Solution (ETMS) and Travel Risk Intelligence Service (TRIS), helping to provide solutions that mitigate operational risk and assist corporations with compliance of "duty of care" obligations.

The tools of the trade were broken down into four headings: **Policy; Training; Monitor; Response.**

Policy.

Policy is your strategy for demonstrating "duty of care". Echoing previous speakers', the development and implementation of your policy is paramount and can be achieved through effective communication. Once in place you can't rest on your laurels; you must amend, update and re-communicate regularly.

> "The immediate 24 hours before this conference had seen 250 incidents worldwide that could disrupt travel"

Training.

Not just for your staff but also your clients. Don't just rely on a booklet and assume they've read it. Use e-Learning and email to communicate your policy.

Monitoring.

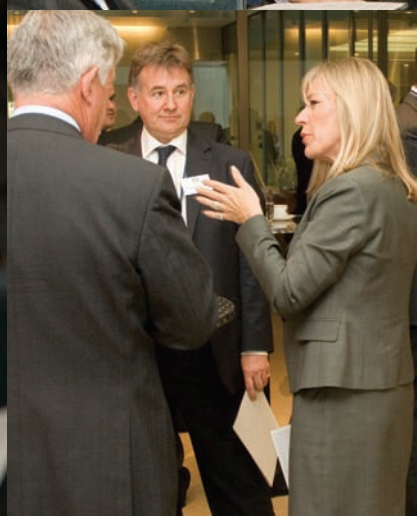
By tracking global incidents you can better understand their potential impact. The day before this conference had seen over 250 incidents worldwide that could disrupt travel. These ranged from earthquakes, severe weather warnings, riots to bombings.

Using ETMS and TRIS allows for the tracking of travellers and incidents. By identifying the traveller, and where they are, means you can get messages through to them. Credit card transactions are useful to follow. Technology, such as digital maps, can help pin-point locations. Likewise, Cell ID which uses smart-phone technology to locate or GPS tracking by mobile phone. A delegate attending from one of the world's leading mining and exploration companies said they used "emanation" bags in China. These bags stopped Chinese authorities from monitoring in-bound and out-bound phone calls. If you can't be tracked by phone, how do you do it? Judge said you need to tailor your tools to where you're going. In the case of China, a dedicated device like a Radio Frequency Identifier could do the same job. Technology is out there to be used. You could even "chip" people as in the latest James Bond film!

"A range of tools, working together, is what's required to achieve faultless, fast response times providing travellers with useful alerts and reports"

Response. Keep it simple. Too much information can be counter-productive: just give what's needed. You don't want to confuse people or panic them. Sanitize what gets out to the traveller. Never forget the power of a phone call. A simple card with an emergency number can work wonders. Human interaction and a consolidated service will deliver an effective service. The fluency of technology used is crucial. No one tool is the most useful. For example, Itinerary Tracking software lets you know where people are and a simple phone call, text or email can advise the traveller what to do. A range of tools, working together, is what's required to achieve faultless, fast response times providing travellers with useful alerts and reports.

Judge neatly summed up when he said; "**Good security is a business enabler**".



Questions

Here are a selection of questions that stemmed from the Q&A:

During the 7/7 attacks the mobile phone system crashed. How can we guarantee communications?

The amount of phone calls overloaded the system, true, but text messages were getting through. In fact this is how the emergency services managed to communicate underground. On land, mobile phone towers were actually disabled so that any other potential bombs couldn't be triggered.

Some clients will want people to travel to see them, but what if the area is a risk?

If the Foreign Office says it is a risk then do a full risk assessment yourselves. Record your findings in case anything goes wrong later. You can shape some things, but there will always be an element of luck. As an employer you will always hold that duty of care, you cannot delegate this to someone else, a consultant for instance.

From a responsibility point of view how does that play out in a law firm environment where you have many partners, all owner managers of the firm?

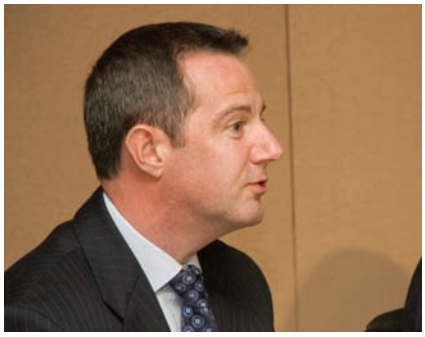
....a lawyer's answer; we're not entirely clear yet! We haven't had a decent case under the Corporate Manslaughter Act that's going to tell us...we need to wait and see how the judges interpret the Act on a case by case basis. However, if the Partners take the decision about who to send where, potentially the Partners or individual Partners are going to be liable in those individual circumstances, not the person who is booking the tickets.

Do we need to increase security or is the balance right?

It evolves with the threat. For example, a community approach to the problem is good as it helps standardise procedures. This creates uniformity, which is good, but too much can lead to predictability and be exploited by an enemy.

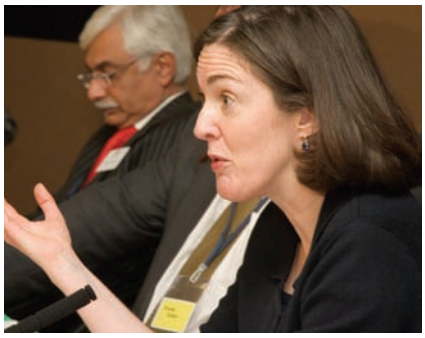
In conclusion, Frank Gardner asked the panel if they thought travel was safer now.

Matthew Judge said corporate travel is not more dangerous, but there is a lot more travel so there is always something that can happen.

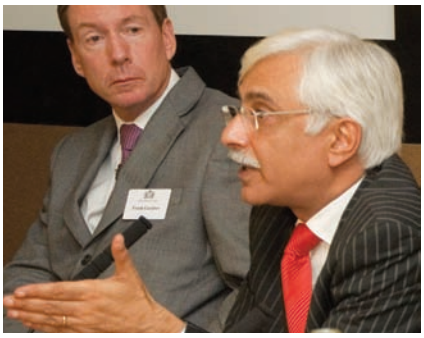


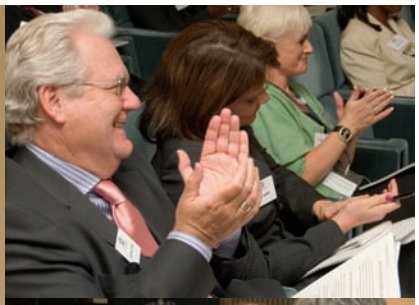
Andy Blackwell stated that travel is safer now and the journey to the airport was probably the riskiest part of a trip! Indeed, anybody can enter an airport unobstructed: it's only from check-in onwards that security measures impinge. Don't do the terrorists' job for them - keep the paranoia down.

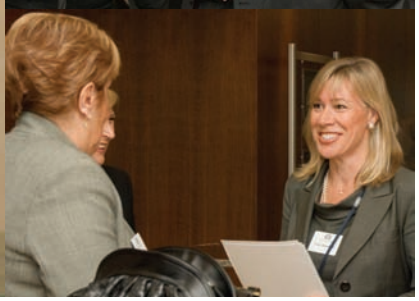
Fiona Gill felt that, regardless of real or perceived risk, stopping corporate travel was not good however there will be more accountability in the future.



Rattan Keswani agreed with Blackwell, but also stressed we must understand why any attack happens; it is to create a sense of fear, dismantle economies and business. Security is better now and we must see any possible threat in that light, we must share experiences.







Closing Address

Richard Boardman, CEO of Reed & Mackay, thanked everyone for attending especially the panel. This debate was all about bringing expertise into the room, experts in their various disciplines, to be thought provoking and to challenge some of the processes that we have in our businesses.

At Reed & Mackay we have always been alert to the importance of traveller safety and security and believe that having invested some 18 months ago in an Incident Management Unit to compliment our 24-hour Emergency Travel Service, we were pushing the boundaries of safety and security management in the travel management community. We believe we are leaders in this field but we cannot be complacent and recognise there are always going to be opportunities to improve upon the standards we have today, to ensure the wellbeing of our employees and make sure their security always comes first.

If you would like further details on the next Reed & Mackay debate please contact **John McKee** on **0207 246 3333** or **johnmckee@reedmac.co.uk**

REED&MACKAY

STRATEGIC TRAVEL MANAGEMENT

Reed & Mackay 26 Old Bailey London EC4M 7QH

T +44 (0)20 7246 3333 **F** +44 (0)20 7246 3255

E reedmackay@reedmac.co.uk **W** www.reedmac.com