COVER FEATURE

TRAVEL SHOULD BROADEN THE MIND, NOT THE RISK

By Stuart Hughes

Overseas travel, particularly business travel, can be seen as glamorous by the uninitiated. In reality, it can be fraught with risk. For those climbing Mount Everest, risk is part of the experience, but for the average business traveller, danger should not be part and parcel of the trip.

It is clear that everybody has a different appetite and perception of risk. Equally, we all instinctively manage risk to some extent day in and day out to ensure nothing goes wrong in our daily lives. Business travel should be no different, both for the traveller and the company. For businesses not to manage risk would be remiss at best and potentially negligent at worst. Whilst business travellers should expect their companies to undertake reasonable steps to ensure they are fully prepared and aware of the risks and how to mitigate them, the business itself should reasonably expect the traveller to heed the advice and training provided.

Reconsidering "Safety"

One could be forgiven for thinking the world is always a dark and dangerous place. For many years we've been increasingly fed on a diet of twenty-four-hour news coverage from channels such as CNN, N24, RT, BBC, Al-Jazeera, and so forth. Many corporate security executives and their operations' teams are professionally tuned into these news sources. This is alongside advice from governmental bodies such as the UK's Foreign and Commonwealth Office (FCO), Germany's Auswärtiges Amt (Federal Foreign Office), and the US's Overseas Security Advisory Council (OSAC) coupled with information from travel security and intelligence providers such as Risk Advisory, NC4, Anvil, Control Risks Group, iJET, Special Projects and Services, Stirling Assynt, Drum Cussac, and MAX Security, to name only a handful of the myriad of expert providers. In the digital age, more contemporary news feeds like those found via social media sites such as Twitter, LinkedIn, and Facebook are very often the first to break emerging stories surrounding incidents. This constant coverage, by and large, reinforces to us that only bad things happen. So it is fair to ask how often we see a positive news story.

Recent incidents have shown to us that it's not only the parts of the world with weak law and order, security, or governance where our employees can be put at risk. We've seen these recent incidents happening in many major European cities, such as Berlin, London, Paris, Madrid, Brussels, and Istanbul, inevitably bringing death and destruction with them. The focus of security executives has, therefore, had to evolve to include cities previously considered "safe."

Recent incidents have shown to us that it's not only the parts of the world with weak law and order, security, or governance where our employees can be put at risk. We've seen these recent incidents happening in many major European cities, such as Berlin, London, Paris, Madrid, Brussels, and Istanbul, inevitably bringing death and destruction with them. The focus of security executives has, therefore, had to evolve to include cities previously considered "safe."

Incidents have also continued to happen in parts of the world long considered challenging environments, parts of the world where businesses—particularly those with a retail dimension—have sourcing, manufacturing, or supply-chain operations. Whilst these major incidents, wherever they may occur, grab the headlines and rightly a significant amount of our collective professional attention, we must not forget the more common incidents that will also regularly impact our colleagues.

The frequency of incidents such as road traffic accidents, petty crime, sexual offences, and illness or injury requiring medical attention is many times greater than those that are the focus of news reporting, as is the probability of travellers encountering such circumstances. How many people travel with prescribed medicines, and how many of those have given adequate consideration to the legality of that medicine in their destination countries or their ability whilst there to acquire the necessary health care for their conditions or replenishment of their medications? The medication point is particularly important. Whilst perfectly legal in the traveller's home country, it may be deemed illegal in the destination country, and harsh penalties can be brought to bear—turning the previously innocent business traveller into a drug trafficker as they cross the border.

How many employees utilise a hired car in a foreign country immediately after getting off a long-haul flight? Is the person competent to drive in that country? Are they well rested? Did they drink alcohol whilst on the flight?

The content of this article is for general awareness and information purposes and should not be relied upon as legal advice. It is beyond the scope of this article to go into detail on every country's legislative framework or to serve as a comprehensive review of every applicable law. But it is my intention as the author, and someone with broad experience of this issue, to raise awareness of what is a critical corporate blind side.

Duty of Care

The broad term used to describe this corporate responsibility is "duty of care," and it is equally applicable to the health, safety, security, and well-being of employees, contractors, and other people the organisation has responsibilities toward. Across a number of countries, both the corporate entity (and in some cases, the parent company) and individuals within the company can be held accountable by the courts for duty-of-care failures.

Any corporate entity is required to robustly demonstrate that it has adequately discharged its duty of care across the full range of incidents from the headline grabbing to the more common. The focus of this duty is often restricted to those employees engaged in business travel. It should not be forgotten, however, that duty of care extends also to local employees, expatriates, and potentially even to their dependents and those residing with them.

All this is set against a volatile, uncertain, complex, and ambiguous world, whilst facing a challenging backdrop of inconsistent global

standards, limited guidance for employers, and an increasingly mobile workforce. As business becomes ever more global and people more mobile, companies are regularly sending employees to far-off destinations with little or no notice to deliver on strategically important objectives. But it must be remembered that none of these extenuating factors diminish the responsibility of the company. The potential implications of any type of incident occurring where the duty of care is not robustly considered and fulfilled include not only lawsuits and resultant damage to brand and reputation, but also the potential to impact the retention of existing and attraction of future employees, students, or brand ambassadors.

Executives will no doubt in the future be called to account for their actions or lack thereof in relation to robustly delivering on the wholly reasonable expectations of employees, shareholders, customers, and relevant legal and regulatory bodies for breaches relating to travel security and risk management. Let's be clear—duty of care is not simply a moral or an ethical consideration or one that should be a matter of course for any "employer of choice"; it is a legal requirement in many European countries. Many of those countries where it is currently not a legal requirement are now reviewing the enactment of such laws.

The duty of care and the corporation's obligation (and that of executives) to organise itself in an appropriate manner is increasingly being used by shareholders as a basis for legal action when a business has, in the investors belief, not adequately discharged its duty of care. Those investors are seeking legal redress to recoup losses related to negative share-price impact.

It is not beyond the realm of possibility that this could be brought to bear in relation to business travel or other security-related incidents impacted by foreseeable risks—surrounding for example launch events or expat assignments, especially where the impacted person is or could be a VIP, brand ambassador, or key member of the executive team. This is particularly crucial if a company has comprehensively failed in its duty of care or there is a significantly negative share-price impact.

Tone from the Top

A notable challenge (as with any topic within a large corporation) is the "tone" from the top, without which there will be little traction. To ensure the correct level of focus, there is a requirement to have strong leadership commitment from senior management up to and including the CEO. This is particularly relevant given that travel risk management and duty of care do not sit in an isolated silo. Rather they span multiple departments within an organisation and require extensive cross-functional work. Signposting this commitment will significantly support the integration with day-to-day business processes and the focus of relevant stakeholder parties. An unambiguous tone from the top will also go some way to ensuring the requisite level of budget and resource, which is imperative to success.

There are key aspects that will support a corporation in demonstrating it is taking its duty of care seriously. These include, but are not limited to, vision, strategy, policy, clearly defined roles and responsibilities, threat identification, risk assessment, prevention and mitigation strategies, incident and crisis leadership, communications processes, and decision-making authority. Clearly the travel security management vision, strategy, and policy must support the corporate strategic direction enhancing the business's ability to achieve its overall objectives. After all, security has the fundamental aim of facilitating the business wherever its risk appetite may take it. The travel risk management strategy in common with the organisation's enterprise security risk management activities should be baked into the business's overall risk management process.

The broad term used to describe this corporate responsibility is "duty of care," and it is equally applicable to the health, safety, security, and wellbeing of employees, contractors, and other people the organisation has responsibilities toward.

Turning to the travel security policy, this should provide a framework for the security objectives surrounding travel, and it is the organisation's opportunity to set out a statement of intent providing the formal outline of what the organisation will do to keep the people it has a duty of care over safe. It is the organisation's chance to clearly state that people should not place themselves in imminent danger nor will they be expected to do so. Such a policy should also address the interactions with other relevant policies within the organisation, for example, incident management or insurance.

Such a policy cannot be written in isolation and must be written in consultation with all relevant stakeholders, particularly those whose responsibilities have ramifications on travel. Furthermore, a key aspect of the policy should be the unambiguous assignment of responsibility and authority surrounding travel risk management. Naturally, as one would expect, the policy should be a living document subject to periodic review at a frequency defined by the organisation, for example taking into account changes in legislation, debriefings post-incident, or changes in the organisation's risk profile.

Companies such as Uber, Airbnb, and the future similar examples not yet conceived further illustrate the requirement for periodic review of policy. Your employees are using them in their private lives and for business. Any policy needs to reflect that reality, whether accepting or restricting their usage. It is also illustrated by the recent travel moratorium implemented by the US. Whether you agree or disagree with it, your policy has to take it into account. The policy and its intent should also be communicated to all relevant parties, respecting the culture both of the organisation and of the individual countries where it is to be implemented.

UK law requires a risk assessment to be "suitable and sufficient." To be so, an appropriately qualified and experienced person—someone who understands the risks and how to manage them—must carry out the risk assessment. This would be a good rule of thumb to follow regardless of jurisdiction. The risk assessment measures the probability and severity of potential harm to the individual. The risk assessment must have an adequate level of detail to be clear and to accurately reflect the situation and activity and to identify all foreseeable significant risks. In short, it needs to enable the responsible persons and the traveller to take those steps that are reasonably practicable in the circumstances to prevent or mitigate the risk. The expectations in this regard, placed on large global corporations, will naturally be higher than the expectations placed on small businesses.

Employee Training

Training for the travellers should be a key component of any travel risk management programme. Once adequate training is provided (and documented), any traveller can carry out threat identification as he or she identifies danger. Proactively empowering travellers by ensuring that they are well prepared and possess greater levels of awareness is an extremely effective way of clearly evidencing the duty-of-care processes. Training will need to cover travellers in general and will also encompass different levels according to the threats and risks identified. Every traveller will need to know the basics, including the scope of the travel security and risk management provision that is in place and how to access it. At the basic level, one example is the knowledge of the telephone number of the retained travel security and medical assistance provider.

Employees should be aware of their responsibilities in the effective management of travel security and the potential impact of their work and their actions. The implications of non-compliance both for the individual and for the organisation should be clearly articulated.

A comprehensive assessment of the training needs should be undertaken. For example, not all travellers will require hostile environment awareness training (HEAT) or security awareness in a fragile environment (SAFE) training courses from companies such as Pilgrims Group, Control Risks, or Precedence Travel Safety and Security. There will also need to be consideration of any specific nuances relevant to the culture of the destination that may need to form part of the training. Training should not be restricted to those travelling but should also include those people who book travel or organise events.

Ongoing Assessment

Having the correct processes in place for both threat identification and for the risk assessment of travel are the fundamental starting points for travel risk management. Profiling both the traveller and the destination is an important factor in the process. There are multiple components that can increase (or decrease) risks for travel to specific locations, including experience of the traveller, age, gender, sexuality, nationality, and culture (of the destination and of the traveller).

> Threat identification and dynamic risk assessment must be an ongoing process. It is not something that can be done once and then disregarded. Threats and risks will change, as will business needs.

These processes should be utilised whether the travel is to low-, medium-, or high-risk destinations. For travel to higher-risk locations, the process should include a justification around the approval given for travel and who made the decision. It is also necessary to consider any existing medical conditions and the required clinical or medicinal treatment. Threat identification and dynamic risk assessment must be an ongoing process. It is not something that can be done once and then disregarded. Threats and risks will change, as will business needs. Adequately addressing the duty of care will only be achieved if such processes are documented sufficiently. The baseline minimum expectations would need to include providing evidence as to the policy, the criteria, the mitigation measures against which the decision was made to permit travel, and who made the decision.

Where risk or threats are identified during travel, processes should be activated that alert and advise the traveller accordingly. It's obviously advantageous that these processes are rehearsed and have adequate internal and external resources applied to them.

Prevention and mitigation strategies should be prioritised, firstly aiming to eliminate the risk entirely. Secondly, where the risk cannot be eliminated, the resulting aim would be to minimise the risk. And where neither is possible, put in place strategies to control the risk. Any such strategies will have to take account of travel destination, travel route, travel methods, travel itinerary, and the traveller profile, thus underlining the dynamic nature of the process, as many of those aspects can be (and often are) subject to change, often at short notice. As would be expected, any mitigation or prevention measures have to be proportionate to the risks faced and the corporate risk appetite.

Incident management training should occur regularly with clear response plans that identify the responsibility and authority levels of those involved alongside escalation protocols. Where the threat and risk levels are deemed sufficiently high, the protocols should include repatriation plans covering all people the organisation has responsibilities for and who can initiate such plans. It is imperative that a communications professional be included both in incident management (IM) teams and any subsequent crisis leadership. It is clearly important that the IM team be fully aware of the organisation's capacity to respond to any incident including any dedicated resources, local support, and external providers.

A key challenge relating to incident management is identifying where travellers are at any given time. Not knowing exactly where impacted persons are when an incident takes place can lead to unnecessary workload, missed opportunities, and increased risk. Providing a level of traveller tracking either by phone-based app or utilising standalone GPS devices is one solution. However, without the correct processes, resources, and training in place, this will provide a false level of comfort.

There is clearly no reward without risk. With the right preparation, planning, training, and risk mitigation, the rewards of business travel for both the organisation and individual can be huge. Happy travels! ■

STUART HUGHES is an experienced international security and risk expert who has worked for a number of corporate brands including sports giant adidas AG, where he was the senior executive responsible for global corporate security. He is now managing director of Enterprise Security & Risk Management Ltd. (ESRM), an enterprise security practice.