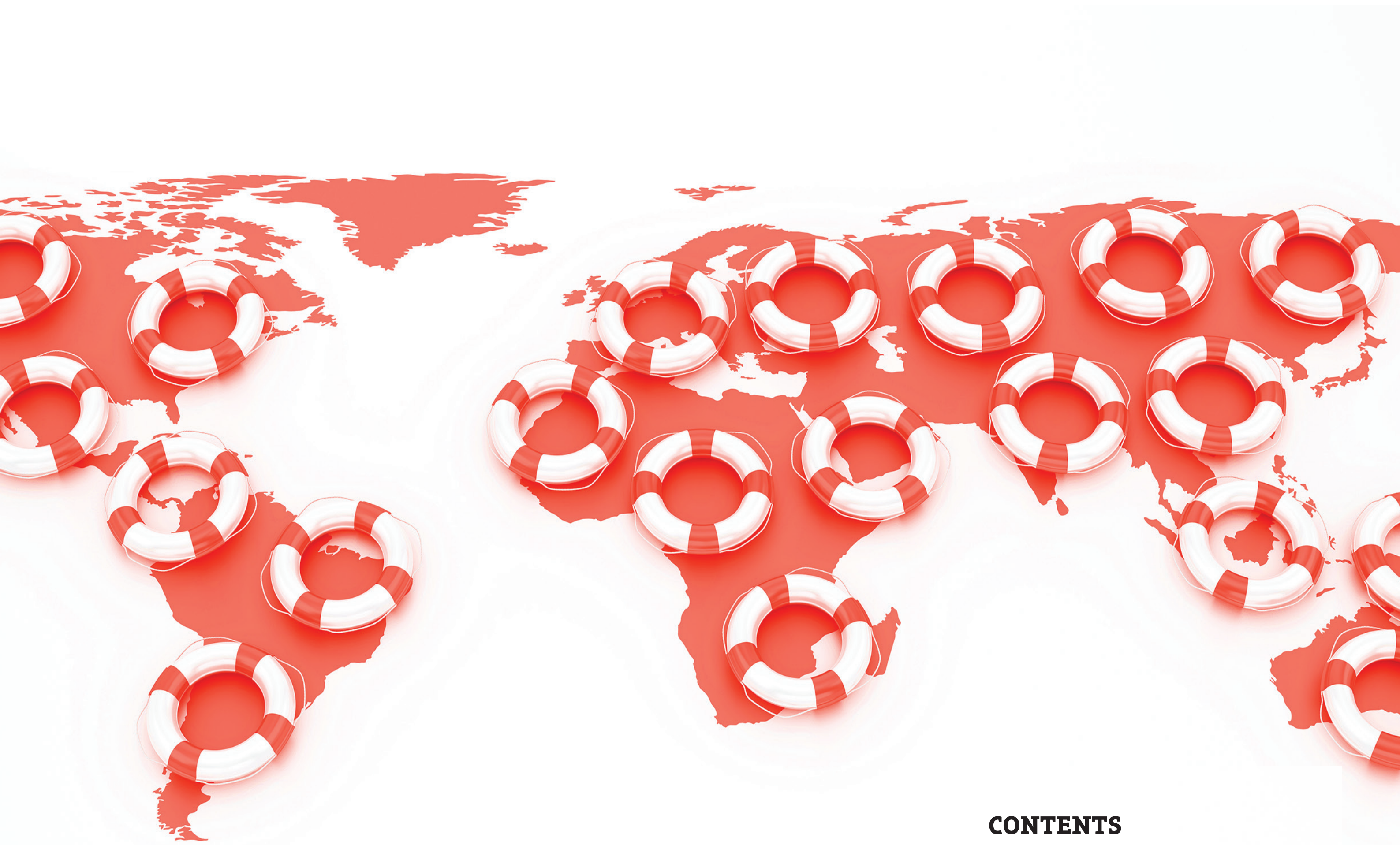
StrategicRISK



SPECIAL EDITION: PEOPLE RISK

IN PARTNERSHIP WITH AIG

CONTENTS

CHANGING RISKS

CRISIS MANAGEMENT

RISK AND HR

TECHNOLOGY

THE EVOLVING NATURE OF TERRORISM

Today's terrorist groups are targeting public spaces, in a bid to create mayhem. We must be proactive in protecting and empowering our people and our businesses.

The attack on a hotel, restaurant and office complex in Nairobi by four gunmen from Islamic extremist group al-Shabaab in January 2019 is a reminder of a familiar modus operandi: the deliberate targeting of people and public places by terrorists. But it's not all so familiar – compared to terrorism in the past, such as the plane hijacking and hostage-taking by Middle Eastern terror groups in the 1970s and IRA bombs targeting government buildings in the 1990s, terrorists' tactics are widening. They are now increasingly taking the form of lone and 'active assailant events' involving guns, knives and vehicles – as well as bombs.

The recent attacks in Paris (2015), London (2017) and Strasbourg (2018) are among those that have deliberately targeted civilians, using vehicles, knives, and guns – creating an addition to the perils of business travel.

The scope of threat

Led by foreign fighters or lone, home-grown recruits, these assaults are localised and focus on public venues – from concert halls, bars and restaurants to airports, train stations, sports stadiums and city pavements. They demonstrate that terrorism risk does not only affect companies and employees operating in less politically stable regions of the world. They show that the scope of terror risks is widening; that the risk profiles of global businesses with a large contingent of expats and travellers are changing.

Meanwhile, geopolitical tensions are influencing and producing new people-related risks. Eighty-five percent of respondents to this year's World Economic Forum's *Global Risks Report* expect 2019 to involve increased risks of "political confrontations between major powers". "Measures to counteract terrorism at airports may not reduce overall societal risk if terrorists simply respond by shifting to new vulnerable targets such as sporting events, concerts and subways," the report observes.

The number of terrorist incidents in Western Europe increased from 253 in 2017 to 282 in 2018, but there was actually a fall in fatalities. The IEP attributes this to increased counterterrorism measures and better surveillance techniques; and the decline in attractiveness of ISIS, its ability to inspire, plan and co-ordinate attacks. It is also likely that the capability of the "Inspired" amateur is less potent than the trained cadre member.

Politics of fear

"Although 2017 saw a sharp decline in deaths from terrorism in Western Europe, terrorist activity still poses a significant security threat," according to the IEP's Global Terrorism Index 2018. "Potential future sources of terrorism include foreign fighters returning to Europe after the collapse of ISIL in Iraq and Syria, as well as the threat of a resurgence of politically motivated extremist violence in both Western Europe and North America."

"The global political landscape is producing new people risk threats and risks," says Paul Mills, senior security consultant at AIG. "Extremist radical, isolationist and protectionist views by newly elected political parties, state-sponsored cyber attacks, the instability of post war political organisations and structures and global markets and sales tariffs conflicts are all feeding the uncertainty that we all face."

"Uncontrolled migration in Europe, Africa, the Middle East and the US are also creating tensions and resentment, and forcing political change," Mills adds.

Prepare yourself

There are several implications for businesses as they seek to protect their people and assets – wherever in the world they may be. Companies need to consider how their premises, their processes and their staff may be exposed and how the nature of their business or location can influence the level of risk that they face.

While the risk of deliberate attack on a business premises remains low, organisations need to think about how they would respond if their people or property were caught up in a terrorist incident or hostage-style attack.

"All of us must accept responsibility for our own security in today's modern world," says Mills. "Most people do not do that. They rely on government or other entities to provide security safety nets for them. Also, individuals are bombarded with information and technology, which distracts them from being aware of the threats they face. So, it's an educational process that needs to start at a grass roots level."

Know what to do

Mills thinks larger organisations should provide a level of guidance and training for their employees and points to the US, where active assailant training has become a common feature for public and private sector companies, along with other initiatives like the Stop the Bleed campaign.

"It's very good that the UK government has launched a programme that provides first aid training and Stop the Bleed style advice," says Mills.

"So, if you were caught up in a London tube attack, for instance, you would know how to respond. If you combine that sort of training with apps that send alerts and information on incidents that are happening in the vicinity of your location, it empowers people to make the best decisions in a dynamic situation."

TIMELINE OF ATTACKS

› 2015 › Paris
A series of coordinated terrorist attacks took place on 13 November 2015. Three suicide bombers struck outside the Stade de France in Saint-Denis, during a football match. This was followed by mass shootings and a suicide bombing, at cafés and restaurants. Gunmen carried out another mass shooting at concert in the Bataclan Theatre. 130 people were killed and 413 injured, almost 100 seriously.

› 2015 › *Charlie Hebdo* offices, Paris
On 7 January, brothers Saïd and Chérif Kouachi broke into the offices of French satirical weekly newspaper, *Charlie Hebdo*. They were armed with rifles and other weapons, and killed 12 people. The newspaper was known for its controversial caricatures of the Prophet Mohammed and the attackers allegedly say they were avenging the Prophet.

› 2017 › Westminster Bridge, London
On 22 March 2017, an attacker drove his car into pedestrians on Westminster Bridge and then stabbed a policeman to death outside the Houses of Parliament. Five people in total died.

› 2017 › Manchester
On 22 May 2017, a suicide bomber detonated a homemade bomb in Manchester Arena, after a concert by singer Ariana Grande. The attack killed 22 people, and injured 116, over half of them children.

› 2017 › London Bridge, London
On 3 June 2017, three terrorist attackers drove a van into pedestrians on London Bridge and launched a knife attack in Borough Market. Eight people were killed in the attack and 48 were injured.

› 2018 › Strasbourg
On 11 December 2018, five people were killed and 11 injured, when a terrorist launched an attack on the city's busy Christmas market, armed with a gun and a knife.

ACTING ALONE

An in-depth examination into the statistics of terror events uncover a clear and disturbing shift in tactics towards lone assailant attacks. Our best defence? Preparation, education, and thinking ahead.

The importance of protecting staff from terror threats is relatively well understood, but those terror risks are fast-evolving – shifting from large-scale terror to localised civilian attacks– causing many risk managers to start questioning the effectiveness of their insurance and risk management programmes.

Terrorist groups are building network structures to facilitate and encourage growing incidences of lone assailant terrorist attacks; and the rate of internationally co-ordinated terrorist plots has decreased.

As a result, risk managers have, increasingly, been making enquiries about the new threat landscape. In fact, in the last few months, one insurer, AIG, has experienced a significant increase in demand for cover in relation to lone assailant shooter events that target mass civilians. While the focus for this type of coverage tends to be firearms related in the US, risk professionals in Europe have been taking note and increasingly considering coverage – but from a terrorism related angle.

The latest statistics suggest that terror groups are making a conscious effort to increase rates of civilian casualties. According to the Global Extremism Monitor's (GEM) 2017 report, 47 Salafist Jihadist groups deliberately killed a total of 6,310 civilians in 2017. And a report by RUSI, *Lone-actor terrorism*, published in 2016, points to a steady increase of such attacks between 2006 and 2016.

Most vulnerable

Soft targets including schools, shopping centres and parks were targeted by most of these groups – "not for their symbolic value, but for the ease of carrying out a successful operation," says NYA, in a report on terrorism trends.

"These include insufficient physical security measures to deter, detect, delay or respond to assailants, generally supported by limited access control or public right of access," it continued.

TRAINING – BE IT ONLINE FOR LOW-LEVEL CATEGORY RISK COUNTRIES OR FACE TO FACE, FOR HIGHER RISK CATEGORY AREAS – IS KEY.

There is also a huge change in the terror tactics used to cause mayhem and fear. According to the 2018 Global Terrorism Index, attacks to infrastructure is the most popular form of terror attack and, over the course of 2017, armed assaults increased the most in number. Bombings and explosions have been the most popular form of terrorist attack since 2002 but have given way to new tactics.

Know your travellers

These are serious threats and managing them requires comprehensive understanding – both of the individual traveller and the risk landscape.

"The disposition of the traveller should be understood: are they over cautious, gung-ho or practically careful?" says Patrick Smith, global resilience leader for Deliveroo and director at risk consultancy, Acumen Advisory. "Understanding exactly how and when they will travel is key and to have laid down processes and procedures is vital. Using specialist organisations to inform decision making is prudent."

Education will only benefit risk processes and procedures, adds Clive Clarke, risk management expert and former chairman of Airmic. "Training – be it online for low-level category risk countries or face to face, for higher risk category areas – is key. Intranet sites should be well populated with links to training and the insurance/risk team [must be] closely aligned with the travel risk management team.

"Our emails with travel details have reminders of what to do, where to go and a 24/7 x 365 number to call. Colleagues are 'tracked' and alerts sent as soon as there are any issues with colleagues asked to respond to confirm their safety."

Danny Wong, former director of corporate risk at InterContinental Hotels Group and founder of GOAT Risk Solutions, believes companies must go a step further to safeguard employees – and businesses need to think carefully about stopping unnecessary travel.

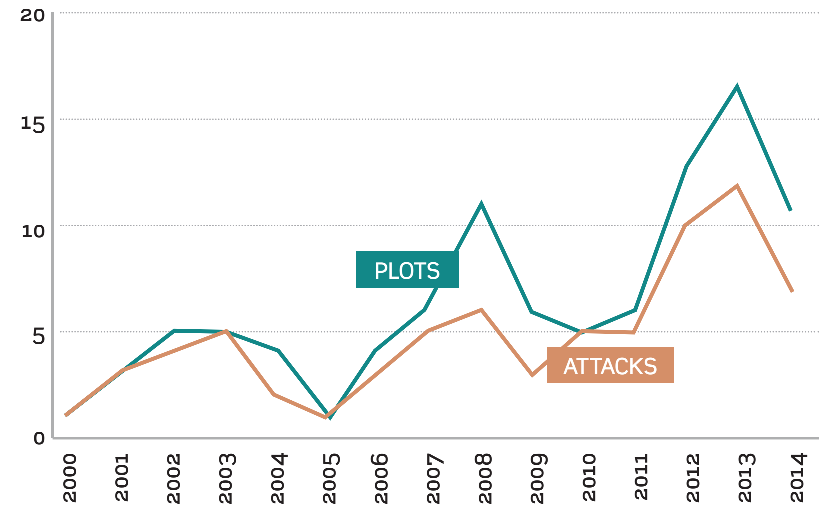
"Most important is to challenge whether the travel was necessary at all," he says. "This is not to say don't go to the emerging market, but perhaps rethink how to enter a new market safely. Examples such as using local partners, joint venture partners or franchise agreements, and employing locals, who are more accustomed to those environments, are often better choices."

But if you must go?

One other crucial partner in the management of terror risk is the insurer. As the threat landscape evolves, they too are rethinking their policies, building into their business travel products coverage for everything from evacuating staff to dealing with hostage situations, and a range of consultative solutions.

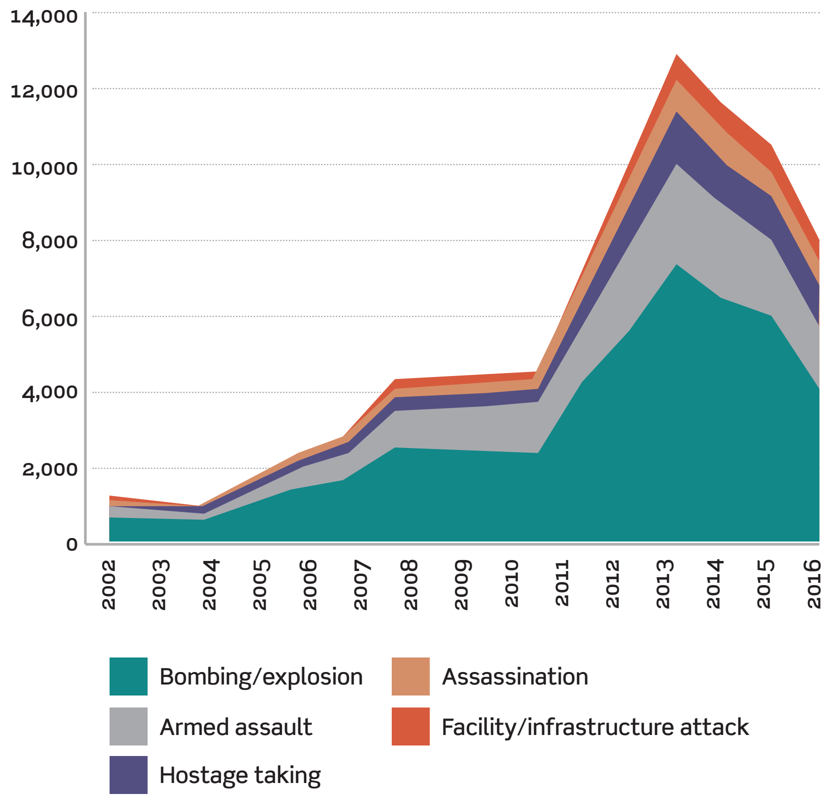
Jon Gregory, global head of crisis solutions at AIG, says: "To be able to deal with these complex incidents and emerging new threats, risk managers expect more from their insurer. So, we are providing more than just financial risk mitigation. They still need the risks indemnified but there's another element – predictive consultancy. This works to predict what could happen and looks for ways to mitigate the risk."

NUMBER OF LONE ASSAILANT PLOTS AND ATTACKS (2000–2014)



Source: RUSI, Lone-actor terrorism, 2016

TYPES OF TERRORIST ATTACK (2002–2016)



Source: START GTD/IEP calculations/Global Terrorism Index 2018

12,500
machines were affected by ransomware NotPetya
20,000
people failed to get medical attention due to WannaCry

THE RISE OF CYBER TERROR

Terrorist groups targeting business and governments with ransomware and data theft could wreak misery and mayhem. But there are ways to armour up.

The terrorism landscape is fast evolving, with perils moving away from large-scale terror to lone assailant attacks targeting mass civilians in localised and public areas. But one other potential shift that has grabbed the focus of counterterrorism groups and governments is the likelihood of large-scale cyber terror attacks and the impact on civilians – both domestic and travelling employees.

The WannaCry ransomware, which infected the UK's NHS and private healthcare in 2017, wreaked havoc on core services. One of the biggest impacts? Some 20,000 hospital appointments and operations were cancelled during the attack – 20,000 people were unable to receive medical attention.

Fortunately, little to no evidence has surfaced of serious or long-term harm to patients' health following the attack, but WannaCry 2017 is indicative of how large attacks of this nature could spiral out of control and have potentially devastating impacts on human lives.

Employers who operate large international assignments must be cognisant of the risks of cyber threats to core infrastructure. Governments, researchers and counterterrorism groups continue to investigate attacks that could affect mass civilian populations. They all agree the threat of a potential cyber terror attack looms large.

As the Centre for Risk Studies at the University of Cambridge and Pool Re, warns in their joint report, Cyber terrorism: assessment of the threat to insurance: "Practices and predictions of terrorists acquiring destructive cyber capabilities date back many years. The National Academy of Sciences first warned of a 'digital Pearl Harbor' as early as 1990."

While no such attack has materialised, the two companies go on to say: "Concerns over the potential movement of terrorism into the cyber sphere endure and, with the broadening of attack surfaces and growing technical capabilities of threat actors, the arrival of cyber terrorism seems ever more likely."

The arrival of cyber terrorism

It is easy to see how such a scenario could become possible. Recent advancements have seen a proliferation of smart technology enter the market place – a trend described as the 'Fourth Industrial Revolution'.

The internet of things, big data, automation, machine learning and artificial intelligence all converge to create hyperconnected networks and a continuum of digitalised operational functions across many industries. The upsides include greater efficiency, which can drive down costs and provide competitive advantage. The downside? An increase in vulnerability to cyber attacks as technologies create new and diverse security challenges.

"The risks are certainly increasing, as are the number of potential types of actors," says Stuart Poole-Robb, group CEO at KCS Group, a cyber intelligence consultancy company. "As such, governments are spending more in terms of time, energy and, of course, money to thwart attacks."

So, what would a cyber terror attack look like? "In its broadest sense, it is an act that is designed to cause panic or terror through damage and destruction," he explains.

"However, it should not be confused with corporate or personal hacking for financial enrichment or industrial espionage, nor should it be confused with cyber warfare against government or military assets."

Instead, cyber terrorism can be described as: "A cyber attack against civilian information, data and systems by terrorist groups or agents related to nation states, whose primary purpose is to sew dissent and uncertainty. It can take many forms and the attack vectors are becoming more complex," he adds.

For the Centre for Risk Studies and Pool Re, cyber terrorism is: "An act of politically motivated violence involving physical damage or personal injury caused by a remote digital interference with technology systems."

Whatever the definition, as WannaCry indicated, large-scale cyber attacks to core infrastructure could halt vital services, have a direct impact on the public and cause panic and disruption.

But WannaCry is only one of several examples of attacks to vital infrastructure that have caused concerns among governments. The NotPetya attack, which first surfaced on 27 June 2017, is another example. The ransomware infected up to 12,500 machines in more than 60 countries, mainly in Eastern Europe. The attack affected critical infrastructure in several industries, including banking and financial centres; energy exploration and production; shipping; terminal operators and other support companies; and power generation facilities.

In fact, A.P. Moller-Maersk – the world's largest shipping company – estimated its losses to be in the region of $200m–$300m, primarily as a result of business interruption.

"As attacks of this type mature, the combined shocks of failing critical infrastructure and economic output put at risk through the unpredictability of international trade and business interruption will have far reaching ramifications," says the Centre for Risk Studies at the University of Cambridge and Pool Re in their report.

As Poole-Robb concludes: "The boundary between government or military assets and private infrastructure companies is becoming blurred as more services become outsourced – causing many more vulnerabilities to a possible cyber terror attack."

FERMA: OUTLINING A PLAN OF ACTION

Ferma has been campaigning for businesses to change the way they operate in a bid to lessen the risks from cyber terrorism and attacks.

In its report *At the junction of corporate governance and cybersecurity*, the association called for organisations to set up dedicated internal cyber risk governance groups to better manage cyber risks, particularly as threats evolve.

The role of the group is to determine the potential cost of cyber risks across the whole organisation, including catastrophic risk scenarios, and to propose mitigation measures to the risk committee and the board.

The association recommends that these groups are chaired by the risk manager but operate across functions throughout the business.

In addition to the risk managers, the group is to be composed of representatives of all key functions involved in digital risk, notably IT, human resources, communications, finance, legal and the data protection officer and chief information security officer.

Ferma president Jo Willaert says: "As recent attacks show, cyber risk is an enterprise issue that affects strategic aspects of the board's mandate, including valuation, reputation and trust. The management of cyber risk has, therefore, become a corporate issue that should be reflected in the governance of the company."

"Our recommended cyber risk governance model constitutes an innovative way for organisations to approach cyber security. It will allow the board of directors to demonstrate that cyber risks are managed on a rational and documented analysis of the risks across the organisation."

But insurers also have a role to play, and their support should be factored into internal cyber governance structures.

Chris Burgess, UK cyber leader at AIG, says: "Whatever the scale of the attack – whether they affect critical infrastructure and halt vital services to the public; or a data breach that could damage consumer trust and tarnish brand equity – cyber attacks are now an inevitable risk for business, support services and core infrastructure, and governments."

"Prevention, mitigation and response requires a strong co-ordinated approach, which brings all internal stakeholders in line – and which is further enhanced by the support of highly experienced cyber and IT experts."

"There are critical providers whose value can be defined by the breath and depth of services that they can offer – expert consultations on effective preventative measures; 24/7 support during the response phase of an incident, including forensic investigations; PR and communications support to lesson the impact on brands and reputation; reliable risk transfers to indemnify losses; and robust claims management."

"And this is where insurers can help. Through a standalone cyber policy, insurers can provide the added support to internal cyber governance structures to ensure they are fit for the cyber challenges of the future."

EXPERT VIEW

THE ROAD LESS TRAVELLED

The modern workforce is on the move. A comprehensive threat response product is needed to keep your people safe from a growing range of travel threats.

Business travel has never been more necessary, with large corporates seeking new markets, suppliers and raw materials in what is an increasingly interconnected world. Travel is growing ever-easier and more affordable, but as it does, this increased global mobility is introducing new challenges and concerns for employers. Chief among these worries is the need to prioritise the safety and security of business travellers.

Traditional medical-related risks remain a prominent threat for business travellers and risks that will always exist, no matter where in the world a member of staff travels. From the less-travelled areas of Western Africa to the more mature business hubs in the US, getting access to timely, reliable and safe medical assistance will always be of the greatest priority.

The well-being of staff can only be met adequately if companies have access to a robust medical network that is available 24/7 – anything less can put members of staff at great risk.

Rocky roads

But, of course, in the new age of international assignments, business travel risks extend beyond the need for quick and dependable medical assistance. Within the macro trends of globalisation and increased global mobility are a range of heightened exposures: natural catastrophes, pandemics, terrorism and political instability among others.

The way in which businesses are expanding is introducing a range of threats, as multinational organisations move into regions that are more complicated and less stable. China's Belt & Road Initiative and major energy and infrastructure projects in the Middle East and South America are just some examples of mass expansion that have contributed to a surge of business travellers and expats – all of whom are travelling during a time of heightened geopolitical tensions and into locations where political instability exists.

At the same time, the terror landscape is fast-evolving, with a growth in workplace radicalisation, violence and 'active assailant events', increasing the need for crisis response, security and repatriation.

These dynamics bring major risk implications, of which employers must be much more alert. First and foremost, there are the aforementioned challenges over employee well-being and duty of care. Then there are other corporate considerations, arising directly from these people and business travel risks – business interruption, brand/reputation and liability issues.

IN THE NEW AGE OF INTERNATIONAL ASSIGNMENTS, BUSINESS TRAVEL RISKS EXTEND BEYOND THE NEED FOR QUICK AND DEPENDABLE MEDICAL ASSISTANCE.

In discussions with our clients, we asked how we can support them as they develop and grow a more international footprint. A modern and mobile workforce requires more than a conventional travel accident policy.

Increasingly, clients are seeing the value in a more comprehensive threat and consultancy response product, which marries the traditional coverage and travel management and medical injury support with a range of intelligence-led and crisis response services.

Answering people risk concerns around the full remit of potential threats – terror, political instability, natural disaster, pandemics and epidemics, and criminalisation – we've enhanced our business travel policies to better respond to the changing risk landscape. It brings together security protection, crisis management, evacuation and repatriation, and medical assistance, all under one umbrella.

A life line

AIG's Lifeline Plus provides clients with a travel assistance mobile app that includes, among other features, a one-touch 'help' button and security travel alerts. It offers security training for business travellers, the latest intelligence and country reports, and an optional Crisis Plus Extension that responds to more than 20 different potential or actual crises, from the criminal to the catastrophic.

For any business travel risk, we want to work with clients to understand their exposures and risk appetite, to offer certainty of cover and access to a global consultancy network that can support them, whatever the threat or concern.

We recognise that today's business traveller is exposed to varying and complex risks, and that the nature of business travel risks is fast evolving. Our new, enhanced product offers peace of mind.

This article was written by:

Ian Robinson, head of UK personal insurance, AIG: IanRobinson.uk@aig.com

Jon Gregory, global head of crisis solutions, AIG: Jon.Gregory@aig.com

CRISIS COMBAT

Effective crisis management is about protecting your people, your assets and your reputation.

In today's globalised and interconnected world, business travel risks extend beyond medical assistance to more complex risks arising from security incidents, natural disasters, terrorism, epidemics, and the ever-growing number of malicious acts to personnel. Set against the dynamic threat environment is a steady rise in business travel and international mobility over the past decade, largely driven by the need to source new growth opportunities abroad.

It is estimated that 6.8 million overseas business trips were made by UK workers in 2017, according to the Office for National Statistics. And some 63% of business travellers believe the threat environment has become more of a concern, according to 2017 research by Ipsos MORI. Security threats are the most commonly reported reason for modifying travel itineraries, followed by natural disasters and country risk ratings.

In any major incident, repatriation, evacuation and crisis management needs to be co-ordinated, fast and proactive. Protecting employee's welfare – particularly risk to life – should be the number one priority. In addition, reputation is vital in international markets, and if organisations' crisis response plans fail, they risk damaging their brand equity.

"It's not only about putting the right risk mitigation measures in place, it's about accepting that you can't fully mitigate risk away," says Tess Baker, director at crisis management consultancy NYA . "Some residual risk will always remain so organisations need to be prepared to respond to adverse events."

"When something goes wrong that affects an organisation's people and their families, there will be media interest and reputational impact," she continues. "You only have to look to the recent attack in Nairobi which turned into a full-blown crisis for many organisations. When something like that occurs, you need to have tried and tested mechanisms in place to stand up and respond effectively."

"Managing a travel crisis requires a 'dual process' that kicks into action when an incident occurs," says Emmanuel Fabin, insurance manager at TSB. "There's a process of managing the risk on the ground as well as managing the risks within the organisation."

"On the ground, there are advice helplines and apps where staff can get real-time updates," he adds. "If there has been an earthquake or terror attack, one of the first things they'll want to know is: what's going on and is it localised or countrywide? How can I get emergency help if I need it? How can I get repatriated out of the country?"

6.8m
overseas business trips taken by UK workers,
2017

Know your priorities

According to Airmic, the four pillars of effective crisis management are: anticipation, prevention, response and recovery. "There are of course decisions to be made about priorities in a crisis," says John Ludlow, chief executive of Airmic and former head of global risk management at InterContinental Hotels Group. "Hopefully boards will conclude that people are more important than property or money."

"Clear leadership, communication and vigilance are needed to ensure that intentions and actions demonstrate integrity when things go wrong," he continues. "Top of the people list of priorities are of course employees, so risk managers need to work with HR to ensure this most precious of corporate assets is well protected."

Primed and ready

By their very nature, crises are unpredictable. But scenario planning and anticipating what could happen – and then training staff to respond appropriately – can help mitigate the risks. This includes encouraging staff to be aware and vigilant of what is happening around them as they travel to and from work or on a business trip; and explaining what they should do and who they should contact if an incident occurs.

63%
business travellers are more concerned by threat landscape

"I've just come back from Australia and I was reminded how many natural disasters happen regularly there, for example major storms and flooding," says Karla Gahan, deputy global head of risk and advisory at VinciWorks and former deputy head of risk at DLA Piper.

IN TODAY'S WORLD, BUSINESS TRAVEL RISKS EXTEND BEYOND MEDICAL ASSISTANCE TO MORE COMPLEX RISKS ARISING FROM SECURITY INCIDENTS, NATURAL DISASTERS, TERRORISM, EPIDEMICS, AND MALICIOUS ACTS TO PERSONNEL.

"For companies with global operations and people in earthquake and hurricane zones, it is a big consideration. You need to stop and think about how you would look after your people if a disaster happens."

CASE STUDY: IN A WARZONE

When an NGO operating in Afghanistan was attacked by six armed insurgents, its insurer AIG had analysts monitoring and responding to the incident as it unfolded. A vehicle containing a suicide-borne IED had detonated at the entrance of the NGO's compound, followed by attackers entering in an effort to maim or kill as many people as possible.

"The analysts quickly picked up, through the various channels, that one of our key clients was going through a sustained and significant armed terrorist attack," explains Paul Mills, senior security consultant at AIG. "This was reported to the broker, the client and myself, and that same day we met with the client in London to provide immediate advice."

Meanwhile, the insurer's assistance team was speaking to local hospitals in an effort to understand whether there were casualties and where they would be taken, in order to co-ordinate air ambulances if needed.

"This was all happening in the first few hours of the client experiencing this traumatic event," he says. "Fortunately for the client, they had practiced being attacked by armed attackers or a bomb detonating on or around their location, and they had a fully equipped safe room to relocate all of their staff."

After 10 hours of fighting, the assailants were neutralised by local Afghan security forces. "Thankfully staff had been inside the safe room during that time with food, water and other supplies to keep them going. We were able to provide advice while the attack was ongoing and had arranged a lot of assets in the background to co-ordinate a medical response and repatriation had the worst happened."

"We also advised them on the need to find alternative operating locations for the company, as well as what counselling support we could provide once the event had unfolded," says Mills.

NEXT-LEVEL COVERAGE

When trouble hits overseas, you need best-in-class incident response – and this requires a new, evolved type of insurance.

When disaster strikes during an international business assignment, the implications for organisations can be huge. If a company responds badly to a crisis – providing inadequate evacuation and repatriation support, for instance – it could inadvertently damage reputation and brand equity. And, the risks could extend from people risks to wider corporate threats – business interruption, share price shock and loss in market share, for example.

Managing such incidents well relies on good forward planning, thorough post-incident support strategies and a smooth claims process.

"More can be done to prevent incidents, combining specialist knowledge with bespoke business and risk understanding, which is why internal risk teams should be best placed to own this area," says Danny Wong, former director of corporate risk at InterContinental Hotel Group and founder of risk consultancy GOAT Risk Solutions.

Support at every step

But in many instances, support from insurers can be invaluable – if the right policies are in place. Against a backdrop of new and complex business travel risks, insurers are evolving their solutions to ensure that support can be offered during all stages of an incident – and not just after. This includes support at the prevention phase; during an incident, in the response phase; and after in the claims management stage.

How well a policy responds in a crisis will depend on the specific insurer and the type of cover that has been bought, as well as how well prepared an organisation is.

"Policies are generally fit for purpose, but their adequacy at the point of need often reflects the skill of the purchase," says Patrick Smith, global business resilience leader for Deliveroo and director of Acumen Advisory.

Insurers have their part to play.

Time to evolve

James Morton, regional security director, EMEA at AIG Travel, says: "The threat landscape is constantly changing, and new problems mean the insurance world has to play catch up. For instance, after the 'Arab Spring', and a series of anti-government protests and uprisings, some businesses were found wanting, in terms of their insurance policies. Insurers struggled to cope with the complexity of the situation.

"Insurance products can't stay as they are – they need to evolve to respond to the threat landscape and client demands. Cover needs to be interlinked, broad and cannot just be responsive. Clients expect support and predictive analysis."

He adds: "Not all policies are fit for purpose with regards to reputation management. Insurers are developing plenty of data on poorly managed crises that businesses never recover from.

"Managing these requires a closer relationship with customers on a broader set of threat concerns, better understanding of the business, and managing reputation throughout a crisis. Innovative products must support indemnity beyond the event itself."

A cautionary tale

One overseas company experienced the benefits of this 'closer relationship' with its insurer when a series of civil disorder incidents affected its stores.

The attacks caused serious threats to the safety and well-being of the company's staff members and customers, as well as major physical damage and loss in assets.

Naturally, the company wanted to plan and mitigate against similar events in the future. It was keen to understand the precise cause of these attacks and identify the triggers and warning signs of future catastrophic crises. It wanted to devise a plan that considered strategically important locations, distribution centres and personnel.

Much of this fell on the company's insurer – AIG – who were called upon for assistance. Through close collaboration, AIG identified the individual retail locations that were affected, investigated and established the reasons they were targeted, and consulted on how the company could be more aware, informed and resilient.

It then examined the business's store locations to determine which were strategically important and which were most vulnerable to such attacks.

Doing the research

The insurer was able provide this level of advice because it conducted a deep-dive analysis of past civil disorders to understand the triggers, looking at everything from local trends and natural catastrophes to elections and even police events.

Using this data analysis, AIG designed an intelligence component that would continually monitor the risk environment, identify when an attack was likely, and warn the client in a timely manner, allowing them to respond.

With this level of detail, the insurer created a benchmark for the company's internal security staff and staff training crisis response programmes for store location managers and the workforce.

Finally, a comprehensive review of financial risk mitigation insurance products was undertaken to make sure the insurance products were completely appropriate.

Morton concludes: "This is a classic example of the evolution of insurance policies today. Now insurance products sit alongside security consultancy to produce unique solutions for clients with diverse problems."

HOW WELL WOULD YOUR POLICY RESPOND?

Situation: Disappearance

A company employee disappears while on a sponsored run around a Mediterranean island. A detailed search by local police cannot locate the individual and no sign of criminality is found. After local media coverage, the client receives a demand for money for the safe release of the individual.

AIG's response:

- Consultant deploys to location and liaises with local law enforcement.
- After investigating, establishes the demand for money is a hoax.
- Carries out a further search of the area using different techniques and establishes the circumstances around the employee's accidental death.

Situation: Workplace violence

A UK company announcing redundancies has threats made against the HR manager. The HR manager also fears she was followed home one evening and receives a number of intimidating silent telephone calls.

Intimidation continues with deliberate damage to the HR manager's car and a threatening letter being received at her residence.

The crisis operations room gives over the phone advice on personal safety at home and in the office, and how to implement practical security measures. They also liaise with local police to make them aware of the situation.

AIG's response:

- Consultant deploys to location, installs basic covert CCTV and conducts surveillance around the office and residence.
- Evidence gathered identifies individual involved, enabling the police to act.

IS YOUR INSURANCE PLANNING FIT FOR PURPOSE?

Risk management expert Patrick Smith gives the top questions risk managers must ask themselves.

- How well has the business and its travel plans been articulated by the broker and policyholder to the insurer?
- Have the claims and crisis response solutions accessible from the insurer been properly reviewed?
- How have the insurance, crisis and incident reporting processes been communicated to travellers; do they know what to do, what's covered and what's not?
- Is the insurance seen as a financial instrument or as access to a highly skilled response team?
- How does the insurance response fit within the crisis management and communication plan, in the event of a major incident? The organisation's reputation is key.

EXPERT VIEW

BEYOND A ONE-STOP SHOP

The pitfalls to buying business travel insurance for employees are plenty. But insurers have taken note and are offering blended but robust and bespoke coverage.

From nat cats, criminalisation, crises, kidnap and ransom to pandemics, travellers are exposed to a growing number of complex risks, extending far beyond medical assistance. So how is the insurance industry helping?

Traditionally, companies would purchase more than one insurance policy to ensure coverage for a range of perils – business travel insurance and medical assistance, crisis insurance (K&R), travel security, and personal accident coverage, for instance.

But without bringing all stakeholders together into a co-ordinated approach before purchasing insurance, businesses remain at risk of buying too much coverage.

Then there is the complexity of ensuring the right providers and services are in place to effectively respond to a travel incident or provide the required assistance to settle a claim. This becomes even trickier when several insurers are involved.

Businesses saw the pitfalls of their travel insurance arrangements following the 'Arab Spring', when a series of anti-government protests, uprisings and armed rebellions spread across the Middle East in late 2010.

Many businesses that needed assistance from their insurers found a lack of co-ordination and teamwork because they had procured coverage from several different insurers – all of whom were concerned only with their own part in the claims process, rather than working together.

Poor communication, different time zones and complex relationships led to many companies feeling frustrated and confused. Even worse, it meant that solutions worked poorly, and in a lot of instances, the claims process was especially hard to navigate.

Work together seamlessly

But insurers are listening. Many have evolved and enhanced offerings, bringing together all relevant policies into one product to better cater for the myriad travel risks – from medical advice and vaccinations to evacuation, crisis cover and security services.

It is critical that risk managers choose a provider with robust infrastructure and best-in-class solutions in all the areas that need coverage. Risk managers need leading crisis insurance, and business travel, as well as an in-house support system.

It is vital that insurers do not just blend different capabilities but build in predictive consultancy and services. The same company is organising your medical treatment on the ground as well as providing security, repatriation, and organising payments and claims processes. Claims teams, assistance and emergency teams must work together.

One number to call

One concern that risk managers have raised is the notion that blended insurance products might mean lighter coverage – but this should not be the case.

Brokers can play a valuable role here. If a risk manager wants to buy one end-to-end travel product, they need to be reassured that, for instance, the crisis insurance element of the cover is as thorough as if it had been bought individually. Brokers can help their clients probe each aspect of the insurance product to ensure that it is fit for purpose.

Moreover, having one team working together is a lot more effective. It's easier to identify the real problems, and a business or staff member only needs to phone one number to get everything sorted.

Internal harmony is critical for end-to-end insurance products to work and businesses need to be reassured that the solutions is truly blended rather than different departments fudging elements of cover together.

For organisations to get the most out of a blended solution, it is equally critical that they work internally to make sure that different internal departments are also working closely together.

It is crucial, for instance, to ensure that relevant departments outside of risk management are aware of the cover and know what the benefits are.

While a risk management team may understand the specifics of a crisis insurance policy, the security team may not. If your security department doesn't understand that the disappearance clause in your cover allows them to spend $50,000 to carry out searches, they won't be getting the full benefit of the solution.

Risk managers must work with everyone from IT and security to HR departments to explain what insurance has been bought, and what is included with it.

Only then, when a product is truly blended and the company buying it is leveraging it properly, can a business truly see the value of end-to-end insurance.

This article was written by:

Ian Robinson, head of UK personal insurance, AIG: IanRobinson.uk@aig.com

IT IS CRITICAL THAT RISK MANAGERS CHOOSE A PROVIDER WITH ROBUST INFRASTRUCTURE AND BEST-IN-CLASS SOLUTIONS IN ALL THE AREAS THAT NEED COVERAGE.

FIGHTING COMPLACENCY

How do you foster threat awareness and guard against complacency among your travelling workforce? We get the lowdown from **Tess Baker, director at crisis prevention and response consultancy NYA** – AIG's service partner in crisis management.

What are some of the basics of prevention and mitigation when it comes to protecting your people from major risks when they are travelling and working abroad?

The first thing companies need to do is properly understand the different kinds of risks their people are exposed to. This varies by operating environment and might include natural hazards such as fires, earthquakes and tsunamis, or man-made events like terrorism, kidnap, political uprising, etc.

Organisations should carry out a threat assessment for the environments they are operating in to help them determine how likely such threats are. This is usually based both on quantitative analysis (using data on past events) and also qualitative analysis, which considers trends and prediction of future occurrences.

Then you can assess how vulnerable your staff are by reviewing the security measures and protocols that are in place, considering the premises they're working in, the accommodation they're living in, how they're travelling around and also any leisure activities.

This helps identify gaps and weaknesses in the organisation's protection, policies and protocols. What's also key is staff adherence to such protocols. You can have all the right things on paper, but if there is poor enforcement or compliance, then people will be still be vulnerable and the organisation exposed.

YOU CAN HAVE ALL THE RIGHT THINGS ON PAPER, BUT IF THERE IS POOR ENFORCEMENT OR COMPLIANCE, THEN PEOPLE WILL BE STILL BE VULNERABLE AND THE ORGANISATION EXPOSED.

How should organisations seek to build personal security awareness among their staff?

There is a lot of free information available that relates both to security and medical threats, such as the advice given out by the UK Foreign & Commonwealth Office. And there are a multitude of subscription services available from organisations like ourselves, which provide very in-depth analytical reports for particular locations or types of threat, depending on what is needed. Another good source of information is from people with direct, recent experience of a particular operating environment.

Organisations then have to find the most effective way of disseminating this to employees. That can vary from automated emails that are sent out when an employee books their travel, through to tailored one-on-one briefings and training sessions.

When it comes to high-risk environments, it is important to engage employees and ensure that information is understood. Individuals who travel a lot and have lived and worked in high-threat environments can become complacent.

We work with many organisations where the employees have many years' experience working in remote and high-threat environments. They have a very high risk tolerance and don't necessarily like being told what to do by their company. There has to be a culture of security and it has to be endorsed and pushed down from the highest level. If the CEO isn't seen to be adhering to sound personal security advice and protocols, why should the rest of the employees?

And then it's about having an appropriate incident and crisis management framework in place. If there is a medical or security emergency, who do employees call? Companies need to make sure a response mechanism is in place to support employees; to get them the best medical care and/or the right advice as quickly as possible. That's a really critical part of this.

Are some individuals more vulnerable than others? How should training be personalised?

When it comes to travel risk management and people protection, you can break down your workforce into different groupings based on number of factors. There are locations where you may be at greater risk based on gender and nationality. Some staff may be more of a target because they carry high-value intellectual property. There are also differences in risk level based on a person's age and experience. So, it's about understanding the variables and scaling the advice and the mitigation measures accordingly to fit the individual.

WHEN IT COMES TO HIGH-RISK ENVIRONMENTS, IT IS IMPORTANT TO ENGAGE EMPLOYEES AND ENSURE THAT INFORMATION IS UNDERSTOOD. INDIVIDUALS WHO TRAVEL A LOT AND HAVE LIVED AND WORKED IN HIGH-THREAT ENVIRONMENTS CAN BECOME COMPLACENT.

EXPERT VIEW

PAIN POINTS OF MEDICAL ASSISTANCE PLANNING

Medical risk planning is not just a nice to have, it's critical for business continuity and supporting employees.

Medical risks continue to be one of the biggest threats to UK business travellers, with international travel exposing them to anything from broken bones and heart attacks to infectious diseases like malaria.

Companies have a duty of care to safeguard employees' health when travelling. It is therefore important to fully understand the risks that employees face when they are on an international business assignment – both medical and beyond– and to know what businesses can do to prevent or manage them in the event of an emergency.

Small risks, painful impacts

Medical-related risks remains a top threat, and our research shows that the most common risks faced by business travellers include:

- Alcohol – Business travel often involves corporate entertainment and client hospitality, which has led to alcohol-related injuries.
- Pre-existing conditions and physical limits – Employees may have issues such as emphysema, which could be exacerbated by certain climates, or mobility issues that mean they struggle with flights of stairs. Equally, medical conditions such as diabetes and high blood pressure do not conveniently disappear when staff are travelling.
- Transfers – Many traumas occur during transfers, e.g., when travellers are getting on or off a bus, navigating airports or taking trains in unfamiliar locations.
- Distractions when walking – Plenty of people get injured because they're distracted when they're walking. A common issue is looking the wrong way when crossing the road.
- Eating exotic cuisine – Not fully understanding what they are eating and how it was prepared can cause stomach issues for employees.

These threats might each seem small, but their impacts can be huge, and companies need to be able to provide a range of solutions, including prevention and advice, access to medical care and on-the-ground doctors, and repatriation support.

CASE: FIT TO FLY

We recently helped a 60-year-old British man on a field trip in Chile. He fell four metres into a riverbed and needed to be transported to the nearest hospital by air ambulance.

The patient sustained multiple breakages to his arms and legs. But the hospital was ill-equipped to deal with such extensive injuries, so he was transferred to another facility.

After arranging direct billing, we called the receiving doctor who said that the patient needed multiple surgeries and at least a week in hospital to aid recovery.

The patient said he wanted to go home for further treatment. We held a phone conference between our in-house team and the treating medical team to decide on the best course of action.

We agreed that medically the patient would be safe to fly home, provided he had a nurse with him and his leg was elevated throughout the journey.

We contacted the patient's preferred hospital to arrange a bed and made his transport arrangements once he was signed off as 'fit to fly'. We secured ambulance transfers to airports, a private nurse, and ensured he had sufficient leg room by booking extra seats for two short-haul flights that didn't have business class options.

The patient arrived safely in the UK, where the nurse conducted a handover to the receiving medical team.

CASE: IT CAN HAPPEN ANYWHERE

In another recent case, a businessman tripped and broke his thigh bone on the way to the airport in Amsterdam. In severe pain, he was rushed to the nearest hospital where the treating medical team confirmed that he had broken his femur and needed surgery immediately.

We arranged a guarantee of payment with the hospital and cancelled his original flight. Post-procedure, the treating medical team became concerned at a lack of movement in the patient's leg so we arranged physiotherapy until he could walk on crutches.

Once he was fit to fly, we started making travel arrangements. He was unable to travel alone so we arranged for his son to fly over to act as his non-medical escort.

We upgraded their seats to business class for additional comfort and arranged wheelchair access and transfers to airports.

Coverage giving peace of mind

Something as simple as getting to the airport can result in a severe injury for an employee. It is vital that all businesses who send staff members abroad have a range of solutions at their fingertips, to ensure that the appropriate medical care can be delivered smoothly, and staff can return home safely.

Working with one insurer who can offer incisive risk advice, medical and security assistance, as well as prevention and mitigation services, will give you peace of mind that the safety and well-being of staff on international assignments are covered by your business travel insurance.

It means that when something goes wrong, your employees have the reassurance of dealing with one team, who can arrange everything from doctor's appointments to repatriation alongside dealing with the claim and arranging payment.

And we can ensure safety and security because we integrate insurance with service, providing an end-to-end solution – from prevention to response, and right through to claims management.

This article was written by:

Ian Robinson, head of UK personal insurance, AIG: IanRobinson.uk@aig.com

JOINING FORCES AGAINST TRAVEL RISK

How HR and risk management departments are working more collaboratively and sharing knowledge to keep their business travellers out of harm's way.

Forty percent of the estimated 500,000 passengers in the air at any given time are travelling for business. There are more people overseas on business than ever before and many more companies are mobilising large groups of workers – sometimes from multiple countries – into overseas work sites and new locations of which they may have limited knowledge of local risks (crime trends, for instance).

This means that there are, potentially, higher numbers of business travellers in harm's way who, naturally, expect their company to provide more than the basic security support plan.

In the age of international assignments, workforce mobility has shifted from an administrative HR issue into a top risk for multinational businesses. Companies are under greater pressure to provide a duty of care and travel risk management strategy that keeps their staff safe, wherever they are in the world, with a recognition that each trip comes with its own, unique risks. This extends to support in the event of an emergency.

Work together

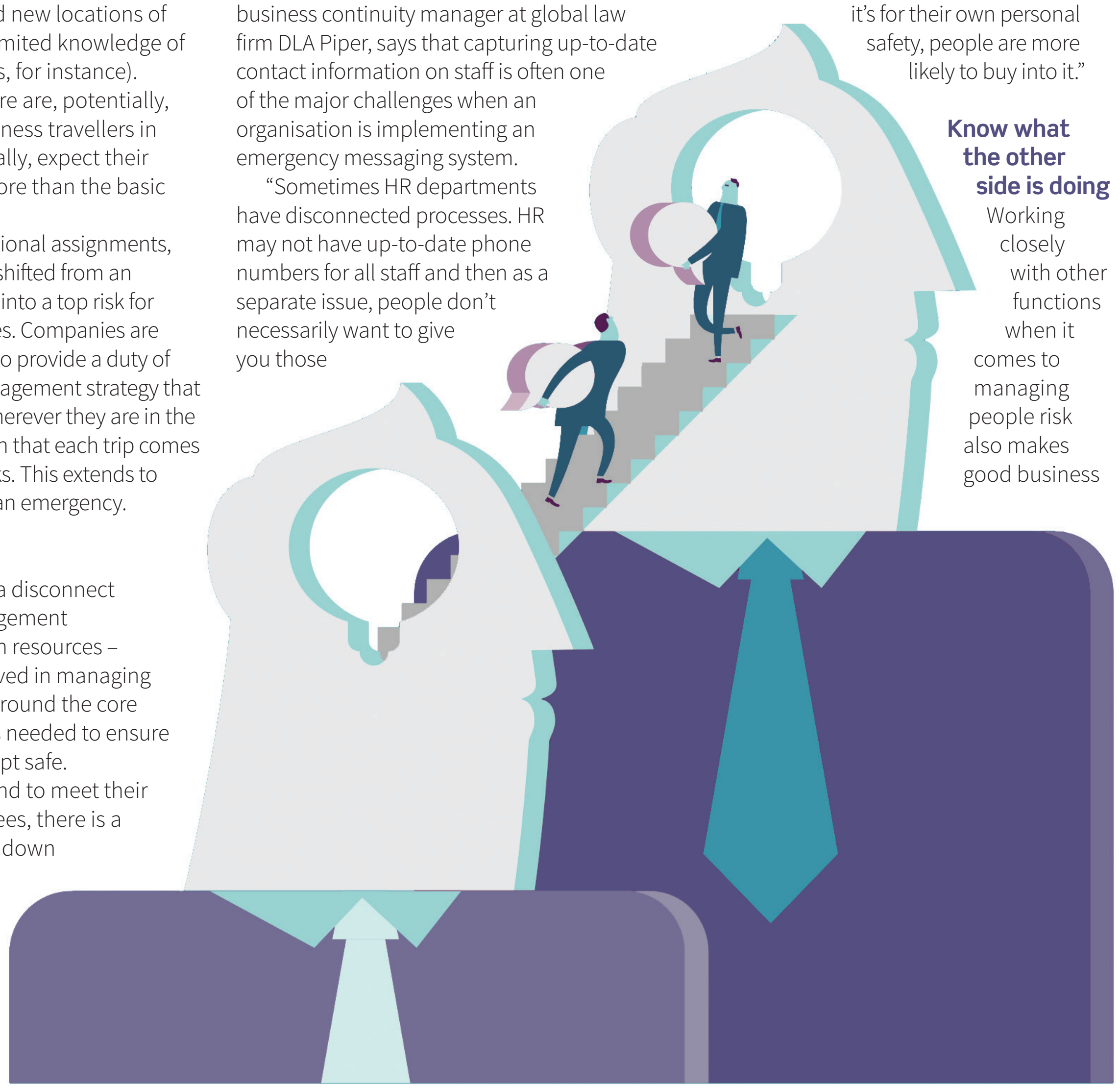
However, there can be a disconnect between the risk management department and human resources – both of which are involved in managing business travel risks – around the core threats and protections needed to ensure members of staff are kept safe.

As employers respond to meet their duty of care to employees, there is a pressing need to break down the silos that exist between HR and risk management departments, which traditionally have operated as separate functions and are governed individually, says Karla Gahan, deputy global head of risk and advisory at VinciWorks. "It's about making sure you have the right relationships, processes and systems in place to ensure you can contact people in an emergency or crisis."

Gahan, who was the former risk and business continuity manager at global law firm DLA Piper, says that capturing up-to-date contact information on staff is often one of the major challenges when an organisation is implementing an emergency messaging system.

"Sometimes HR departments have disconnected processes. HR may not have up-to-date phone numbers for all staff and then as a separate issue, people don't necessarily want to give you those personal details, perhaps for privacy reasons."

"It comes down to communication," she continues, "and this is where risk professionals have got a huge role to play in making sure the organisation's messaging around travel safety and security is communicated clearly and concisely. Once they realise it's for their own personal safety, people are more likely to buy into it."



AIG TRAVEL HIGHLIGHTS CORE TRAVEL RISK STEPS

> Plan ahead and be prepared
It is important to understand the potential cultural, legal and security issues in the locations you are visiting. Not knowing, or disrespecting, local customs might cause you to be the recipient of aggressive behaviour from locals.

> Documentation and accommodation
The cultural and legal climate should be carefully considered, including when booking a hotel or resort. Some circumstances may require a LGBTQ couple to reserve a room with two beds, instead of one, or applying for visas as single individuals if they are a married LGBTQ couple. For women, some hotels offer women-only floors and staying in a well-known and reputable hotel is strongly advised.

> Safety, security and health
Consult a doctor before travelling to obtain specific travel health recommendations and vaccinations, and medical clearance as required. Travellers should also keep all medications in their original containers and carry an official note of medical authorisation from their doctor.

For security reasons, it is usually better for an LGBTQ traveller to stay discreet at all times, even in more accepting areas, to avoid drawing attention.

If you are harassed, remove yourself from the situation as quickly as possible and do not escalate by confronting your harasser. If you believe you are being followed, look for a busy establishment to enter.

Know what the other side is doing

Working closely with other functions when it comes to managing people risk also makes good business sense, believes Emmanuel Fabin, insurance manager at TSB. "It's important to have transparency and communication so there's no duplication of effect. You need to have a more holistic approach to managing people because if you've got different teams doing different things you can undermine the effectiveness of the service being offered to staff."

He gives the example of keeping HR informed when groups of employees are caught up in an incident abroad. "If they're going to be stuck there for several days, this is going to have an impact on the business and all the different functions within the organisation need to be aware of that."

Some organisations are beginning to make inroads, however, showcasing the benefits of aligning the two departments on business travel risks.

Sarah Sandbrook, head of talent consulting and initiatives at Deutsche Telekom, says her organisation learnt a great deal from major events such as the 9/11 terror attacks and the Icelandic volcano eruption and subsequent ash cloud.

"We have a group security and risk team, so if there is a major incident, they'll swing into action, and they're always there to provide guidance and support," she says.

"When there is something like [9/11 or the volcanic ash cloud] and you're talking about the impact on a global organisation, then having a consistent response and the weight of the business behind you is invaluable. Risk managers evaluate all kinds of risks and having them there to swing into action has is one of the benefits of a large organisation."

"For smaller organisations, [HR] are having to [manage the incident] on their own and that can be quite a scary proposition."

Unique risks

Specific advice may be needed for certain groups of travellers who face unique risks, including women – who account for 40% of business travellers – and LGBTQ individuals. This is another area that calls for closer collaboration between HR and risk management departments.

RISK PROFESSIONALS HAVE GOT A HUGE ROLE TO PLAY IN MAKING SURE THE ORGANISATION'S MESSAGING AROUND TRAVEL SAFETY AND SECURITY IS COMMUNICATED CLEARLY AND CONCISELY.

According to a Women's safety survey commissioned by AIG Travel, 45% of female travellers feel less safe or much less safe about travelling than they did five years ago; and 84% reported that their employers either did not provide travel safety tips or that they were not aware of any such tools.

Special considerations will also need to be given for LGBTQ business travellers. According to the International Lesbian, Gay, Bisexual, Trans and Intersex Association, there are 72 countries where homosexuality is illegal and in eight of those, homosexuality is punishable by death.

Moreover, as little as 11% of LGBTQ respondents to a 2014 study by Community Marketing Inc, indicated that they would be willing to visit a destination with laws that restrict LGBTQ rights; and 32% of LGBTQ travellers feel they are treated differently due to their sexuality when on holiday, according to The World Tourism Organization.

These findings culminate to suggest that a travellers' personal profile including their gender and sexual orientation can change the risks that they face – and organisations must ensure they brief all business travellers with appropriate safety tips.

Sandbrook agrees that HR managers need to work with risk management departments to deliver safety and security messages.

She said: "It's about risk awareness and making sure that from an employer point of view we're fulfilling our duty of care obligations. That if we're sending people abroad, we're making sure they're going to safe destinations or making sure they have safety briefings."

Of course, new medical, reputational and security risks have long sat within the purview of risk managers, which is why greater alignment between teams make sense.

And risk managers need to learn from HR teams too, particularly when it comes to the more human sides of risk. For instance, the psychological issues that come with moving staff abroad, or the talent acquisition and retention strategies that are needed with new operations.

The human touch

Sandbrook concludes: "You need to nurture and build talent in the markets where your growth is coming from."

"There's been a huge change in the way resources are recruited managed and deployed. A typical manager 20 years ago would have a team sitting outside their office. Now they have direct employees, contract employees and people working nearshore, offshore and remotely… but you have to bring them together in a team.

"People can quickly become isolated and finding ways to check up on your staff if you're a virtual manager is crucial."

She adds: "Ignore the human element at your peril."

CREATE A ONE-TEAM CULTURE

Risk and HR departments have to put politics aside, break down the silos, and focus on delivering the best advice to their employees.

In most businesses, HR and risk management sit, operate and are governed as individual departments.

But as global mobility increases and many more businesses deploy staff overseas for international assignments, there has never been a greater need for the two departments – each with varying involvement in people-related risks – to align on business travel risks.

Without doing so, companies could, unknowingly, create costly gaps in insurance coverage, adding to confusion over what is and isn't covered.

"There is, of course, the fear that the risk and HR teams are not aligned," warns Patrick Smith, global resilience leader for Deliveroo and director of risk consultancy firm Acumen Advisory. "Without a concerted approach to risk, the matter of 'ownership' is likely to get in the way of the most effective processes."

Exposing gaps and double-ups

He adds that silos between the two departments could "lead to confusion or misunderstanding as to what's covered, what's not, and potential gaps". It could also have an impact on how effectively risks are retained.

Danny Wong, former director of corporate risk at InterContinental Hotel Groups and founder of GOAT Risk Solutions, agrees. "Organisational silos and office politics do sometimes get in the way of good common-sense risk management."

"The result is that employees may not be given the best risk advice reflecting specific circumstances. The latest developments and other control/safety activities may not be taken to the appropriate extent."

Other challenges range from confusion over when claims need to be triggered to concerns about possible duplication of cover.

"There is a risk that overlaps in risk management could lead to duplication of policies and doubling up of cover," warns Emmanuel Fabin, insurance manager for TSB. "This can be mitigated by open communication between functions, and corporate-focused insurance management rather than function-orientated goals."

Companies will only benefit by breaking down silos and fostering greater teamwork – the alternative could put travellers at risk.

Christopher Box, EMEA HR consulting lead at PwC, says: "Organisations are beginning to address people-related risk issues in a more holistic way – but there is a long way to go. HR, risk, compliance and other related functions need to work together to develop complementary policies and broader ways to engage and communicate with employees to truly address risk."

HOST A PEOPLE RISK WORKSHOP, BRINGING HR AND RISK MANAGERS TOGETHER TO DISCUSS ROLES AND RESPONSIBILITIES, ALONG WITH THE CHALLENGES EACH DEPARTMENT FACES IN TERMS OF MANAGING THE THREATS.

If we all worked together...

So, what can the two departments do to strengthen their collaborative approach?

Fabin's advice is for HR and risk managers to: "create stakeholder relationships". This will ensure greater understanding of each other's role in managing people risk – "from both an insurance and people resource perspective".

Another tip is to host a people risk workshop, bringing HR and risk managers together to discuss roles and responsibilities, along with the challenges each respective department faces in terms of managing the threats.

Smith says: "The workshop will create the 'one team' culture, flesh out what each function is doing and can do, and, importantly, create a single approach and voice on the management of people risk and the actions required should an incident or event occur."

For example, travel costs may be cheaper if the team travels together – and this may be the preference of staff – but it could also create a risk. A workshop could trigger a conversation on the risk of all senior executives travelling together.

The start and end point, though, is devising a coherent framework. "It is essential that there is a people risk crisis management plan," says Smith.

"This will reinforce responsibilities, break silo mentality and ensure that matters are dealt with in a clear and concise way," he concludes.

AVOID A TUG OF WAR

HR and risk departments may both be seeking to protect employees from conflict overseas, but they must beware the conflict among themselves.

We've all heard the phrase 'too many cooks spoil the broth' and this is never truer than in business. If too many people are trying to manage the same task, it could lead to conflict and disagreements, if roles and responsibilities are not clearly defined.

One area where this problem can crop up is when managing the risks associated with business travel. This is an issue that tends to involve various departments, including risk managers, HR, security teams and IT.

The myriad functions involved often have different goals and objectives, and this can lead to conflicts around deciding how situations should be managed.

A HR director may have been tasked with bringing down the costs of business travel, perhaps by booking less expensive hotels or travel arrangements, while a risk manager's remit is to minimise the risks associated with business travel, which could lead to costlier accommodation or flights.

Emmanuel Fabin, insurance manager for TSB, says: "At a high-level view, HR and risk are both looking at resource management. [But] HR is looking principally at management of human resource and risk managers are looking at broader management of financial, physical and human resources."

Julia Graham, deputy chief executive and technical director at Airmic, says: "This conflict can lead to accumulation risk, which is about having more than two C-suite members on the same aircraft or a whole team on the same train. You have to sit down with HR and talk about accumulation of risk. Ask: 'Do you realise that you're making people under or uninsured by not thinking about risk aggregation?'"

Time to compromise

It is important, therefore, to understand the different roles and responsibilities that each department may have and where the conflicts may lie. Otherwise, organisations may end up exposing business travellers to unnecessary risks.

And, as Graham notes, this can have far-reaching consequences. "If you negligently allow people to travel and they get hurt, you could face an action."

But bringing together the varying views of several stakeholders will be tricky and the success of this depends on how sophisticated an organisation is.

Sarah Sandbrook, head of talent consulting and initiatives at Deutsche Telekom, has had experience aligning the HR view with the risk manager's view.

"I think the traditional HR view has always been about workplace risks. So most [risks] have been office-based issues, such as trips and falls, etc. But now, the sorts of [risks] you have to think about have evolved. For instance, a few years ago, aircrafts were grounded because of the Icelandic ash cloud. Suddenly HR had to consider: who's stuck, have they got enough money, what's the risk to them as individuals and us as a business?"

Overcoming the potential conflicts requires businesses to break down the silos between the different departments.

Graham says that how you frame the conversation can make a huge difference in getting different departments to work together more effectively.

"My route is to avoid saying that this is my job and instead focus on the need to work as a team. We need to keep the board, the C-suite, employees, people's families and others we are responsible for safe. Say to HR: 'You know the company policy but we know how to put it in into practice.'"

Channels of communication

Communication is critical here. Fabin says: "There can be differences in approach to business travel-related risks within the same organisation but these differences become an issue when there isn't clarity, transparency and awareness. Simply put, you can't resolve what you don't understand or know exists."

Joseph Frederik, EMEA operations manager for security risk management consultancy A2 Global Risk, adds: "There is always this risk, and this is largely down to issues with communication and direction. One way a company can avoid these issues is to centralise the overall risk function and have proper, dedicated representation at board level."

"A former colleague of mine, who worked for a global apparel firm, had a project that could have caused some friction with the HR department. A decision was made to change the access control system at one of their facilities, and this project fell under the security department. This colleague felt compelled to notify HR about this but was questioned by his supervisor as to the need.

"It was very simple. How would you feel if you showed up to work one day and your access card did not work? You may feel that you had lost your job for no given reason. Multiply this by 200 employees, and you will have an HR issue on your hands."

Graham agrees that a centralised policy is critical and should be best practice in any business environment.

She concludes: "Have one travel policy for the organisation, not several. To the employees, the differing roles and responsibilities between HR and risk management should be irrelevant. They don't care who wrote what so long as they know what they should do and where they can go, and there's a procedure in place for if something goes wrong."

OVERLAPS COULD LEAD TO DUPLICATION OF POLICIES AND DOUBLING UP OF COVER. THIS CAN BE MITIGATED BY OPEN COMMUNICATION BETWEEN FUNCTIONS, AND CORPORATE-FOCUSED INSURANCE MANAGEMENT.

SMART AND CONNECTED

The newest technology, in the shape of mobile apps and GPS tracking, means security and protection is in the back pocket of employees travelling on business.

Employers have a duty to ensure the health, safety and welfare of employees, and this extends to members of staff who are travelling abroad for business purposes. Using technology via smart applications, employers can stay connected to their business travellers so that if they get caught up in an incident, reasonable steps can be taken to safeguard and repatriate them.

Natural catastrophes have the potential to affect huge numbers of employees. For a disaster that can be tracked in advance, such as a windstorm, business travellers can be alerted in advance and flights rearranged to take them out of harm's way. In extreme situations, for instance in the aftermath of major earthquakes affecting infrastructure, helicopters can be chartered to rescue stranded employees.

40%
organisations send advisory emails to staff travelling overseas

Hand-holding device

Helping large multinational organisations keep track of myriad staff operating around the world is a new generation of innovative mobile apps and GPS systems. For businesses operating in high-risk locations – including oil and gas, and NGOs – the technology is offered by insurance and travel management firms, giving real-time alerts to incidents as they unfold and a lifeline to staff if they get caught up in an incident.

At TSB, the fall back is always to ensure that another member of staff is aware of a colleague's travel plans and itinerary, explains the bank's insurance manager, Emmanuel Fabin.

"We encourage our staff to download the app our insurer offers but also to have a dialogue with their own line management, so there are at least two people within the organisation who are aware of what is going on with that particular person's travel arrangements. It's about using the technology available but also encouraging people to be proactive and transparent in their communication."

While the idea of Big Brother-style 24-hour surveillance does not sit well in all circumstances, for employees operating in high-risk environments the ability to switch on a GPS tracking system is increasingly appropriate. Several offer real-time tracking, interactive country maps and reports that show travellers by location and date, booking details and pre-trip analysis.

Four in ten organisations have introduced advisory emails for staff that are travelling abroad, in an effort to better inform them about travel risks, according to Ipsos MORI.

Waiting in the wings

For the majority of travellers, the aim is to be helpful but unobtrusive… until a crisis occurs. "When we had the Nepal earthquakes, we had over 200 people that were involved, so we worked with the helicopter companies that we know in and around Nepal to fly in and get people off the mountains," says James Page, chief administrative officer of AIG Travel.

"And then we chartered an aircraft to fly into Nepal to transfer our people to India so we could then book them onto commercial flights home."

The approach to travel risk management should be tailored to each company's risk profile and risk appetite, Page adds.

"Most apps send information to their employees to help them prepare for their travel and the locations they will be visiting. Some have a travel tracking capability so that if an event were to occur, the employer is able to look online and see which of their business travellers may be impacted by that particular event."

"Other perhaps less intrusive tools allow travellers to push out confirmation that they are safe along with their location to their selected contacts."

For business travellers that need emergency assistance, a single touch of a button on the AIG app will connect them with a 24/7 service centre that has medical, travel and security specialists on hand to provide support there and then."

WHILE THE IDEA OF 24/7 SURVEILLANCE DOES NOT SIT WELL IN ALL CIRCUMSTANCES, FOR EMPLOYEES OPERATING IN HIGH-RISK ENVIRONMENTS GPS TRACKING SYSTEM IS INCREASINGLY APPROPRIATE.

Even in Western cities, travellers can find themselves facing a security threat with the need for immediate advice.

"During the Paris riots a client called who was travelling in Paris for work," says Page. "They had gone out to dinner with colleagues but managed to walk into a moving protest. That person stepped into a store nearby and called our centre and said, 'what should I do, where should I go?'"

"Our security team stayed on the phone with that individual while they explained the situation and what they were seeing outside the window. They were then given step-by-step directions to take them back to safety."

Old but good

Of course, mobile apps need a mobile signal or Wi-Fi to operate. In circumstances where neither of these is available or when a battery cannot be charged, the advice is to fall back on 'old' technology, such as land-based phone lines and fax machines.

It is in these circumstances that pre-emptive training and preparation should come into its own, argues TSB's Fabin.

"If you've provided your staff with details of the nearest contact points, whether a consulate or local branch office, and advice on what to do in an emergency, you just have to hope they can get themselves to a place of safety while the organisation attempts to make contact."

THE APP: YOUR NEW BEST FRIEND?

Such new technology offers a 24/7 connection with employees abroad, streamlines the claims process, and can provide critical evidence in the event of an incident.

Businesses have a duty of care to protect their employees when they are travelling abroad for work. This can involve anything from insuring against medical emergencies and lost luggage to protecting against more thorny and dangerous risks – pandemics, terrorist attacks and hostage situations.

Risk managers will want to do all they can to mitigate the risks, from prevention plans and business travel briefings to risk transfer. With the right insurance programmes, there is the reassurance of 24/7 support services, evacuation and repatriation help. And, of course, financial compensation to indemnify companies in the event of a claim.

Support at your fingertips

Triggering and managing a claim typically involves questionnaires and forms but many risk professionals see further potential in travel apps: the possibility of using information gleaned from these applications to support claims management.

This is yet to be seen, and the concept would need to comply with data protection laws, but the upshot is, if this were possible, it could transform claims management in the future.

"Technology, including apps that can measure data and provide claims trends, could help stakeholders to manage claims and become more efficient at identifying and resolving claims issues," says Emmanuel Fabin, insurance manager at TSB.

They could also provide crucial details of a claims incident, says Joe Frederick, operations manager at A2 Global Risk. "Investigations into claims rely on evidence. Apps are designed to geo-locate the user with a high degree of accuracy, and this could be crucial evidence for investigations into terror-related cases."

TECHNOLOGY, INCLUDING APPS THAT CAN MEASURE DATA AND PROVIDE CLAIMS TRENDS, COULD HELP STAKEHOLDERS TO MANAGE CLAIMS AND BECOME MORE EFFICIENT AT IDENTIFYING AND RESOLVING CLAIMS ISSUES.

Whether this becomes a future functionality or not, there is no doubt that there are several benefits of travel apps, most notably, their contribution to the safety and security of employees. So, it is crucial for employers to encourage all staff to use them. But this can be challenging.

You need buy-in

One approach would be to mandate the use of travel apps as a core requirement for high-risk destinations. "A company has a duty of care to its employees, but equally, that employee has a responsibility to comply with policies that are intended to ensure their well-being," says Frederick.

"There are companies out there where, for a trip to get signed off by management, particularly to destinations where the threat levels exceed a company's thresholds, that employee may be required to read a pre-travel brief, go through security awareness training and/or agree to use an app [with geolocation facilities] during their trip," he adds.

For this approach to work, risk managers need to up their marketing efforts and emphasise the key messages: travel apps are aimed at ensuring their safety and well-being.

Bespoke apps, which provide tailored information to risk managers and HR personnel and other stakeholders, will likely be more popular and better demonstrate to line managers the value of marketing the benefits to travellers.

"The key is for insurers to create an interest or desire for travellers to access the app," says Fabin. "One way to possibly improve take up is to have apps that are tailored to certain criteria for corporate and employee preference."

Business-wide statistics would, undoubtedly, interest all stakeholders involved in people risks and duty of care: how many employees are travelling at any given time; number of journeys, mode of travel, and hours spent travelling. An overview of potential claims incidents would also be beneficial – delayed flights, lost luggage, or the need of medical assistance, for example.

An easy sell?

"The better the app, the better it will support the organisations delivery of its responsibility to travellers," says Patrick Smith, global business resilience leader for Deliveroo and director of risk consultancy Acumen Advisory.

He says apps that deliver training, information or advice are an easier sell for HR and risk managers.

"The more apps are geared to risk/travel advice and emergency response, the better they will be. Of course, the app needs to be integrated with the way in which employees are managed/supported by the company, too – they are all too often standalone and are not really used by anyone other than the most frequent travellers."

IN TECH WE MUST TRUST

No matter how sophisticated, security technology only keeps people safe if they use it. How do you ensure staff engage with the tech you develop?

Briefing employees who are travelling for work is critical for businesses to meet their obligations to keep people safe. But duty of care extends far beyond just employees – it includes all stakeholders – partners, directors, contractors – and more: family, students, aid workers, for example. This is one of several steps outlined in Airmic's travel risk management guide.

Julia Graham, deputy chief executive and technical director at Airmic explains: "Oversight is also often with health and safety or security which may or may not be part of risk or HR. And it is essential to work with everyone with a stake in duty of care."

She adds: "You have to brief people before they even contemplate travel. Employees, stakeholders, partners, contractors and family members need to know you have a business travel policy, not just insurance. It's a duty of care you owe people.

"Everyone must familiarise themselves with the policy before a trip, and when people do travel, they should consult those guidelines and contact HR and risk managers or whoever may be nominated by the organisation as 'policy owners'.

"They should also keep reviewing the policy. It's no good someone saying, 'I looked at it last year'. People need to check every time they are considering travel, in case the policy has changed. The world is volatile, and the degree of risk can change quickly."

She advises risk managers to use the BSI standard, *PAS 3001 Travelling for work—Responsibilities of an organization for health, safety and security—Code of practice* as a starting point; and that organisations with people travelling to high-risk countries should work with external consultants to deliver briefings and sometimes bespoke security.

Crisis management and response procedures during and following an incident on an international assignment is also a key consideration and should be built into all centralised business travel policies. She adds: "Some countries may seem lower risk, but parts of a country can be higher risk – you cannot assess risk purely at a country level. Also, risk can be influenced by what you plan to do in-country and who for."

And business travel apps, she says, can be very beneficial. "Travel apps with geolocation capabilities can give a clear indication of an employee's location, which can be incredibly useful if there is a problem.

"Take the attacks in Paris, as an example. If organisations use travel geolocation apps, they would be able to see who's in the country, where they are and use this information to help check that they're accounted for.

"Geolocation should be part of business continuity plans and organisations should be encouraged to use them. Cases like the recent attacks in New Zealand show that staff can go to the most innocuous places, but companies will still need to know where they are and that they're safe."

Tailor it

Travel apps could also be used as a pre-travel briefing tool. Travel safety information can too generic and perceived to be irrelevant to employees, says Danny Wong, former director of corporate risk at InterContinental Hotel Groups and founder of GOAT Risk Solutions.

But if businesses build in processes to flag when a staff member is travelling to a high-risk area, useful information and training could potentially be delivered to them via the app:

"The trouble with travel risk knowledge is that it is quickly out of date, and not bespoke to local towns, or specific conditions of individual travellers or business. Generic knowledge is available on the internet so employee perceived value is low.

"Nevertheless, businesses can put in place centralised travel purchasing policies that have automatic triggers for high-risk travel plans."

IF COMPANIES USE TRAVEL GEOLOCATION APPS, THEY WOULD BE ABLE TO SEE WHO'S IN THE COUNTRY, WHERE THEY ARE AND CHECK THAT THEY'RE ACCOUNTED FOR.

TRAVEL BRIEFING CHECKLIST

All staff travelling abroad must be thoroughly briefed to ensure their security and safety. Patrick Smith, global resilience leader for Deliveroo and director at risk consultancy Acumen Advisory, offers his five-point checklist.

> Know who books business travel.
- Do they understand the cover?
- Do they know limitations (e.g., excluded territories)?
- Do they have up-to-date traveller and family contact details?

> How do you provide key information to the smart phone?
- Does your travel company have an app?
- Does your insurer have an app?
- Do calendar entries include emergency numbers?

> Does the "travel pack" have all relevant information?
- Basic cover detail
- Emergency numbers
- Next of kin details
- Proof of insurance
- Basic advice on security and emergency situations
- Basic information on the destination:
  - Threats/risks
  - Relevant crime
  - Local customs, legal and behavioural requirements
  - Key contact details in an emergency

> Create a cover matrix to determine what coverage applies:
- Business travel
- Personal accident
- Employee benefit-related insurances
- K&R

> Simulate events to determine the following:
- What if there is no access to a phone and/or network?
- What help and support is needed by the traveller?
- How the organisation will be informed of an issue?
- What does the traveller's family need to know and how will this be done?
- How can emergency funds be secured?

StrategicRISK

IN PARTNERSHIP WITH AIG

CONTACT AIG
Ian Robinson, head of UK personal insurance, AIG: IanRobinson.uk@aig.com

Jon Gregory, global head of crisis solutions, AIG: Jon.Gregory@aig.com