



TRAVEL SAFELY

Rodger Cook, Kate Fitzpatrick and Frank Harrison examine the current security challenges facing the global traveller

International travel in 2024 is at a pivotal crossroads, eagerly anticipated by travel enthusiasts, businesses and governments alike, yet facing greater risk and uncertainty than in living memory. Travelling teams face numerous risks in today's dynamic landscape. Economic instability, environmental risks, geopolitical factors and societal shifts all present uncertainties. Cyber security threats like data breaches and ransomware attacks also pose financial losses and reputational damage. The impact of these risks varies across industries, locations and organisations' circumstances.

In this complex global security environment, the importance of diligent research and preparation prior to embarking on travel has never been more critical. Assessing the security and political landscape of destinations and equipping travellers with useful knowledge about potential dangers are essential steps in minimising risks to ensure that business critical travel can continue seamlessly.

The resurgence of right-wing politics, hybrid conflicts and geopolitical uncertainties add complexity

to international travel. Misinformation campaigns are also a growing tactic in hybrid warfare, prompting the need for travellers to stay informed about geopolitical developments using reputable sources.

For instance, Houthi attacks in the Red Sea and territorial disputes in the South China Sea are causing uncertainty and diplomatic disquiet. Around 90 percent of global goods travel by sea, but the risk of geopolitical disruption to maritime routes is extreme.

Border tensions, sanctions and diplomatic disputes can all disrupt travel plans, emphasising the need for robust security measures, up-to-date intelligence and contingency plans for all travellers.

Last year has been confirmed as the warmest since records began, driven by climate change, causing increased frequency of natural disasters. Already this year, we've seen wildfires in Chile, Argentina and Columbia, a powerful earthquake in central Japan, tornadoes in the United States and volcanic eruptions in Iceland. Extreme heat is set to continue in 2024. From hurricanes to floods, these events pose threats to travel schedules, safety and finances.

Protests, civil unrest, terrorism and political instability can cause potential harm and disrupt plans

It is important that, where possible, travel plans have contingency measures in place to safeguard travelling teams to alert them to potential dangers of extreme potential weather or natural disasters.

Emerging needs for new resources to support the energy transition, supply chains and manufacturing have led to a shift in the destinations that business travellers must consider. Places once regarded as high-risk or no-go zones are now unavoidable destinations for many. Travellers and organisations must make informed choices and plan safe journeys to destinations that may have seemed unconventional in the past. While the desire for unique and immersive experiences remains a driving force, we recognise the critical need to ensure safety and security while navigating these evolving landscapes.

Local expertise and experience is key to mitigating the risk when visiting these destinations. Not only should this prepare the traveller for what they can and should expect, it should also include a cultural and society briefing including how to behave, body language and respecting the culture of the destination, the potential risks and ways to avoid them.

Organisations face a constant risk of cyber attacks, particularly when they are on the move, including rising cases of state-sponsored attacks, identity theft, financial fraud data breaches, ransomware targeting critical infrastructure and AI-driven phishing campaigns. These threats can result in significant financial losses, reputational damage and regulatory penalties.

For example, when using public wi-fi networks in airports, hotels or cafes, travellers are at risk of data breaches and identity theft. Hackers can intercept sensitive information, such as log-in credentials or financial details, leading to losses and privacy breaches.

Smart cities, which use technology to improve efficiency and quality of life for residents, are also vulnerable to cyber security threats. For instance, hackers can exploit vulnerabilities in smart city infrastructure, such as traffic lights or public transportation systems, to cause disruptions or accidents. This poses risks to residents and travellers visiting these cities who may rely on these systems for transportation or navigation.

To mitigate cyber security risks while travelling, travellers should use secure networks, such as a Virtual Private Network (VPN), to protect their data. They should also avoid clicking on suspicious links or providing personal information online. Additionally, organisations should educate their employees about cyber security best practices and provide them with the necessary tools to protect their devices and data while travelling.

Health crises, exemplified by the COVID-19 pandemic, have brought forth several risks and changes in travel dynamics that continue to impact travellers in 2024. The pandemic has upended traditional travel practices, making once-popular activities like crowded events, large gatherings and public transportation riskier due to the potential for virus transmission.

The impact of staff shortages in all aspects of the travel ecosystems also remains with chronic delays, restricted customer-facing services and rapid adoption of technology to fill these gaps creating further traveller frustrations and disruptions.

The pandemic has also highlighted the importance of agility and preparedness in swiftly responding to health crises. Future health crises could disrupt

business operations, supply chains, and economies, underscoring the need for organisations to have robust contingency plans to ensure business continuity and financial stability.

Physical safety remains a paramount concern from theft and pickpocketing to robbery and mugging. Protests, civil unrest, terrorism and political instability can also cause potential harm and disrupt travel plans. Travellers need to stay vigilant and well-informed to navigate such situations and safeguard their mobile and computing devices that are often their primary forms of financial transactions, travel itineraries and communications. Keeping valuables at home and dividing cash and credit cards across multiple pockets or bags are simple ways to reducing the risk

SECURITY STRATEGIES MUST BE ADAPTIVE, FORWARD-LOOKING AND HOLISTIC

The human factor in travel security encompasses the need for a security-aware culture within organisations and the crucial mental health aspect for travelling workers and teams. Travellers may face a range of stressful experiences due to the uncertain nature of travel, therefore establishing and maintaining support systems which prioritise mental health and well-being is essential.

For example, being caught up in a natural disaster, dealing with a health emergency or facing a security threat, like a terrorist incident, while travelling can be highly stressful and traumatic. Travellers need access to assistance support that can provide safety protocols, access to medical facilities and evacuation support.

To conduct a comprehensive travel risk assessment for employees, start by determining the trip's purpose, destination and activities. Organisations must know their travellers, their travel experience, and their resilience. Research the country's or region's safety and security conditions, considering factors like political stability, crime rates, terrorism threats, health risks, natural disasters and local laws.

Organisations also need to understand the activities the traveller will perform and if those activities pose a risk from a legal, customary or local cultural perspective.

Check official government travel advisories and review corporate travel policies. Evaluate the employee's personal risk profile, transportation mode, trip duration and communication options. Consider the employee's unique requirements or vulnerabilities and consult local contacts for first-hand information.

Analyse the impact on work responsibilities and establish risk mitigation measures. Communicate risks and strategies to the employee, monitor the situation and provide ongoing support to ensure travellers on the ground are kept informed about potential threats and the impact on their safety is constantly evaluated.

Travellers should also be informed on local laws, customs and cultural norms to avoid misunderstandings or conflicts, and they should prioritise their health and safety by staying updated on vaccinations, carrying necessary medications

and following basic hygiene practices. They should also be prepared for emergencies or have access to travel assistance services. Engage and have the right stakeholders involved. Remember, involving relevant stakeholders, such as human resources, legal teams and security personnel is crucial in the travel risk assessment process to ensure comprehensive and well-informed decision-making. Also conduct a post-travel evaluation for improvement and involve relevant stakeholders throughout the process.

While this year presents unique global travel challenges, travellers equipped with the right knowledge and tools should be able to confidently navigate these uncertainties. Security strategies must be adaptive, forward-looking and holistic. Security leaders should adopt a multidisciplinary approach, collaborating across sectors and borders to address emerging threats effectively. This collaboration

is essential for enhancing security and fostering innovation, resilience and ethical considerations in the face of global challenges.

It is crucial to have a Travel Risk Management framework in place to ensure organisations recognise and mitigate traveller, destination and activity risks. By implementing these frameworks, organisations can better mitigate the risks inherent in today's global travel landscape and protect their travellers. For instance, this includes staying updated using trusted travel advisories, leveraging technology for cyber security, and understanding local customs and laws to ensure a safe and enriching travel experience.

The world is more interconnected than ever, offering unprecedented business opportunities, cultural exchange possibilities and personal growth scenarios, and with the right preparation and support, informed travel is safe travel ●

Rodger Cook is General Manager – Global Security Services, **Kate Fitzpatrick** is Security Director EMEA and **Frank Harrison** is Security Director Americas, at World Travel.

WHAT SHOULD A TRAVEL RISK ASSESSMENT INCLUDE?

Security leaders need to understand who their travellers are as well as where they are going and what they are doing to identify and manage risk exposures. Once the potential risks are identified, businesses should use the model of Educate, Locate, Communicate to prepare the Travel Risk Management programme.

Travel Risk Assessment Inclusions:

Destination Analysis: Identify specific travel locations, considering political, social and economic stability, ongoing conflicts, civil unrest and natural disasters.

Current Situation Assessment: Evaluate destination stability, including health risks, healthcare availability, vaccination requirements, recent outbreak, and epidemics.

Security Analysis: Assess crime rates, terrorism threats and overall safety.

Transportation Risks: Evaluate safety and reliability of local transportation options.

Cultural and Social Factors: Understand local customs, traditions and cultural norms.

Environmental Risks: Assess weather conditions, climate patterns and geographical features.

Legal and Regulatory Considerations: Understand local laws, regulations and customs impacting travellers.

Infrastructure Assessment: Evaluate essential services like communication networks, electricity, water supply and emergency response systems.

Emergency Planning: Develop contingency plans and protocols for emergencies.

Communication and Reporting: Establish communication channels for travellers to report whereabouts and safety.

Personal Considerations: Consider the specific needs and vulnerabilities of individual travellers.

Insurance Coverage: Review travel insurance policies for adequate coverage.

It is vital that travel plans have contingency measures in place to safeguard teams to alert them to potential dangers of extreme potential weather or natural disasters

