



Traveler Tracking & Risk Management Solutions

NBTA Travel & Meetings Risk Management Committee
August 2010

Introduction

References to September 11, 2001, are so prevalent in travel risk and security documents as to be ubiquitous. Unfortunately, subsequent acts of aggression – such as Mumbai, Indonesia, or London – make globalized terrorism close and personal for all travel managers. As we approach a decade since September 11, it is necessary to reflect on what was, what is now, and what is necessary to continue tracking and reporting travelers to ensure the due diligence and duty of care components evolve as the business needs and environment changes.

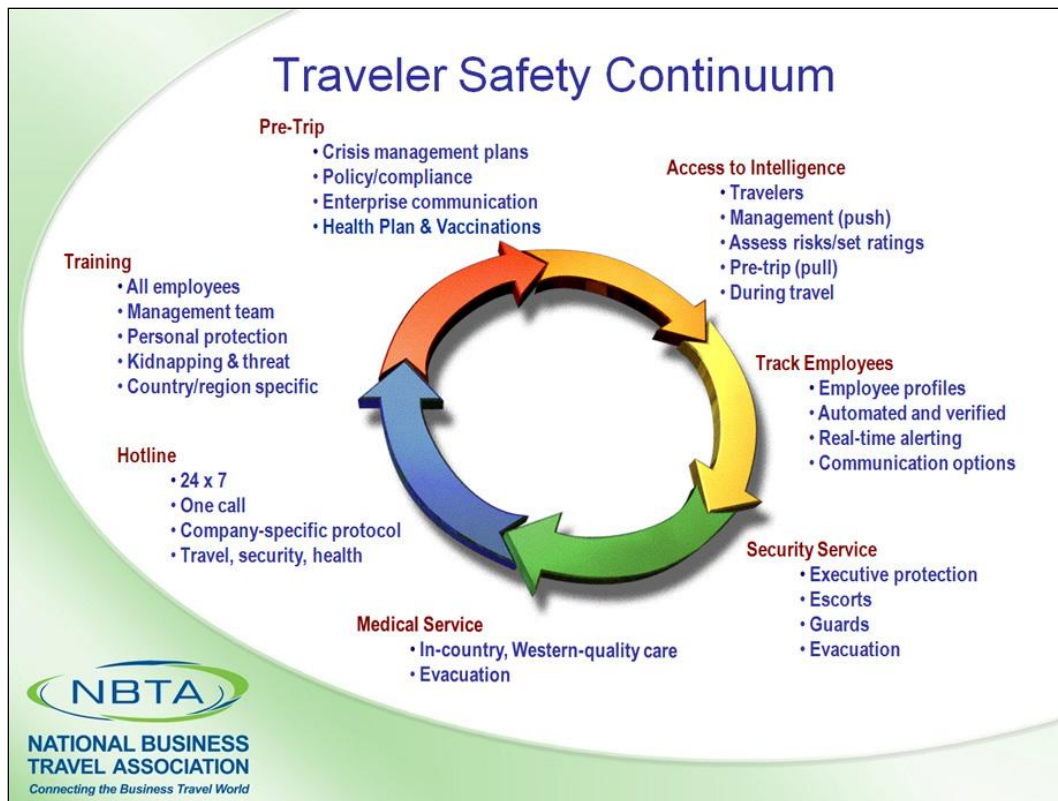
On that horrific day, many corporate travel managers were required to identify who was in New York or the vicinity and contact them, as well as confirm if any employees were on United Airlines flight 175/93 or American Airlines flight 11/77. By 9:25 a.m., the FAA had grounded all domestic flights; and it was necessary to secure alternate accommodation or transportation for stranded travelers. Reliance on Global Distribution Systems (GDS) technology and management level communication were compromised or challenged. The need for qualified and specific information mounted as the day progressed. Many companies had not considered domestic response planning and many corporate travel managers and security personnel experienced fear and panic as they realized their inability to deliver this critical information. It is important to remember that at this time, many companies did not have a managed travel program or an integrated security protocol. There were only a few tracking software programs or centralized data repositories. Travel management company (TMC) reporting was limited and could not be manipulated easily, forcing reliance on GDS data that did not include online or direct system data. These and other related challenges later led to the resulting changes with regard to tracking and risk management within many companies.

Lessons Learned

The staff, reputation, operational assets, financial, and business operations of most companies were at risk. Financial investment and senior level management involvement into systems and operations were necessary to mitigate these risks. In most affected companies, emergency preparedness was incorporated into the various levels of activities; all sought to affirm that their organization was proactive versus reactive. A number of security programs and tracking tools were developed by established and newly created vendors. These options provided a plethora of individual components and comprehensive plans.

So where are we today? Vendors can now provide solutions to collect information across multiple travel providers with the ability to manipulate data, push and pull information, manually enter data external to a GDS feed, and provide assistance regardless of the situation. Organizational needs vary extensively and, in most cases, require flexibility as businesses expand and divest regardless of location. While many companies have initiated or mandated security protocols and travel policy compliance, incorporated emergency response planning and procedures, and implemented a tracking mechanism, the evaluation of such programs must be consistent and ongoing.

What is your role and responsibility with regard to traveler tracking and risk mitigation? Who are the stakeholders, and are they engaged? What options are available, and do you have the right program? Can it do all that is needed to in a time of crisis? This paper will focus on the questions to ask, explain who to engage in the process, and provide a resource guide for the development or enhancement of a tracking component within the Traveler Safety Continuum.



From the *Traveler Safety Continuum* paper, July 2007, available to NBTA Members at <http://www.nbta.org/TravelerSafetyContinuum>

What Does My Organization Need & How Do I Know?

Before determining what solution options are necessary or currently used, a risk assessment should be completed. This is not an independent exercise to be completed by the travel manager in isolation; the engagement of key stakeholders is vital. Cross-functional input is necessary to ensure all potential risks are identified, categorized, and mitigation plans documented. This exercise should be conducted annually or more frequently as the business changes. Key stakeholders should include, but are not limited to, Legal, Human Resources (HR), Security, Travel, Public Relations (PR), Medical, Communications, Technology, Operations, Global Mobility Managers, and Senior Level Executives. In smaller companies, there may not be a designated representative in each of these functional areas. In this case, consideration of possible risks will need to be identified and discussed as a team

For detailed information on assessing your program, read the NBTA paper *Travel Risk Management Maturity Model™ (TRM3™)*, February 2009, available to NBTA Members at <http://www.nbta.org/TRM3>.

The TRM3 model will help you assess ten (10) key process areas (KPAs) related to your travel risk management program. These KPAs include:

- Policy and Procedures
- Training
- Risk Assessment
- Risk Disclosure
- Risk Mitigation
- Risk Monitoring
- Response
- Notification
- Data Management
- Communications

Each of these KPAs are rated on a scale of 1 to 5, with 1 being “Reactive” (lowest) and 5 being “Optimized” (highest). Then, the overall TRM program is scored as the lowest KPA score –a program is only strong as its weakest link -- with a “Plus” value indicating the number of KPAs rated higher than the lowest KPA. For example, a program might be rated a Level 2 Plus 6.

Once the risk assessment has been completed, it should be clear what additional solutions are required to address any potential risk or situation.

Range of Product Solutions

Tracking and reporting solutions currently on the market can be placed into three general categories. These general categories are expressed as solution levels:

Level 1 - PNR/Itinerary Reporting Systems – These solutions represent either existing pre-trip reporting systems or reporting systems that have been specifically retooled to support crisis management reporting.

Level 2 - Reporting systems with Integrated Content – An extension of the traditional pre-trip reporting system with additional content integrated into the reporting. Some of these solutions offer “push” technology of route trip-specific information to the employee.

Level 3 - Risk Management Systems – Turnkey systems and software that address crisis and travel risk management processes and database integration requirements rather than just reporting. These systems focus on both proactive (preventative) actions as well as response management.

Level 1: PNR/Itinerary Reporting Systems

Virtually every TMC can provide some level of pre-trip and ticketed travel reporting service. This type of service captures itineraries when they are created and/or booked (i.e. PNRs) and saves them into a database. While these systems were originally designed to provide travel management reporting, most have been extended with additional reports to support the need for travel tracking. These reports should be web-based and accessible on a 24/7 basis and enable you to view and print within parameters such as “who is traveling today” or “who is flying to what city/country”.

The key advantage of a Level 1 solution is that it is low cost and generally included within the TMC contract.

The key disadvantages are that these systems were never intended to provide real-time or near real-time information. Most existing reporting systems rely on daily or weekly batch file updates to the database. As such, in the event of a crisis, the reporting system will likely not have accurate data, thus potentially creating gaps in reporting. Another disadvantage may be if you have multiple TMCs supporting your organization, as integration of data from various systems is difficult to facilitate. In addition these reports may lack critical emergency contact information and other crisis management information, such as details on a traveler's business unit. Finally, these systems are passive (manual push and pull); usually there is no proactive notification capability.

Realizing the limitations of this type of reporting, some TMCs now offer alternate, third-party systems at an additional cost. It is important to identify and confirm the TMC solution you currently have.

Level 2: Reporting Systems with Integrated Content

The next evolution of reporting is the integration of destination content and the ability to “push” this information to the traveler based on the individual's itinerary. These products require an itinerary (PNR) to be created within the system. In some cases, this is a manual process; others get batch or real-time feeds directly from the TMC and/or GDS.

The key advantage of these products is that they enable the organization to have a proactive travel risk management program that does not require manual review and push requirements. In addition, these systems typically have query and reporting capabilities more tailored to crisis management. Be careful to understand the process necessary to enter the data to ensure real-time data. If your requirements are primarily for travel in low-risk environments, this solution may be all you require. Remember, enhanced third-party options are generally available to fulfill additional requirements.

The primary disadvantage of these systems is that they are not a total risk management solution. For example, this level of solution does not perform an automated risk assessment of the trip and proactively notify the organization if a risk threshold is exceeded or specific issue is identified. Most solutions are “trip-centric” rather than “traveler-centric”. A trip-centric solution stores itineraries and does not link them to a specific traveler profile. A traveler-centric solution links trips to a traveler profile supporting historical travel reporting, first time traveling internationally notification, messaging history, and other benefits. Traveler-centric (i.e. profile-based) solutions generally have the ability to report critical areas such as emergency contact information, medical details, historical travel, trip profile, etc.

Level 3: Risk Management Systems

Risk Management Systems represent the third level of “traveler tracking” products. Level 3 solutions provide capabilities to monitor any world situation that poses a threat to travelers, track employees – travelers and expatriates – and support real-time, multi-modal, two-way communication to all or a select set of employees. These systems were built to be risk and crisis management tools – they did not evolve from basic PNR reporting requirements.

The key advantage of risk management systems is the level of integration of both users and information. The systems support day-to-day travel compliance, global monitoring, exception reporting, and more, with minimal or no manual interaction. When an incident or crisis occurs,

the system becomes a global platform to ensure that employees, managers, and outside response vendors all have access to the same critical information. Since the organization implements and owns the system, it becomes the organization's central repository of information from multiple TMCs and globally dispersed employees.

The disadvantage of a comprehensive, enterprise system can be initial cost and effort required for implementation. Companies that operate internationally, especially in high- to extreme-risk countries, should have a comprehensive travel risk management system to fulfill the organization's duty of care obligations and the traveler safety continuum requirement.

Selecting a System

What type of solution level is deployed within an organization depends on the outcome of a risk assessment, organizational culture, and management commitment to the due diligence and duty of care to travelers. Typically, there is no one product or service that can assist with all potential risks facing an individual organization. Travel tracking and risk management systems form only part of the controls, treatment strategies, and mitigation plans in the event of a situation. It is not uncommon for organizations to use a variety of services and products to support their travel risk management program. It is equally important that designated users become adept at generating critical information from any system and that key stakeholders are aware of the capabilities.

Critical Considerations

After a risk assessment has been completed and before initiating a formal RFP process, it is important to develop a list of requirements necessary to evaluate potential travel tracking and systems. The following list of critical components sets out many of the top-level requirements and is provided as a guideline as you develop your own customized requirements.

When evaluating various travel risk management and traveler tracking solutions, there are a number of critical considerations. These critical considerations are based upon discussions with various travel managers that have utilized a range of tools for a major crisis such as the recent European ash cloud event. Using this event as an example, travel managers became more acutely aware of the critical capabilities and components needed in the time of a crisis.

1. **System Availability and Response Time** – During a crisis, you need the system and data to be available to you and the system to have a reasonable response time. Have your IT department verify the vendor's infrastructure for redundancy and capacity, as well as data security.
2. **Data Completeness** – During a crisis, you need all of your data. It isn't sufficient to report, for example, that 20 people are in Europe when there are actually 27. Can your solution aggregate data from all your sources – TMC feeds, GDSs, low-cost carriers, online booking sites, manual trip registration, etc. Does the solution capture hotels and rail segments? What about passive segments?
3. **Data Accuracy** – Having the wrong information doesn't help you or the organization. While this is an end-to-end process issue (agent to TMC to GDS to TRM vendor), does the TRM

vendor monitor data quality and provide tools to help ensure the highest quality data? Does the vendor provide reporting or work flow to specifically identify trips (PNRs) with errors or possible issues? What about code-share flights?

4. **Organizational Structure** – When you are dealing with multiple business units and managers, you need to be able to slice the data to provide them information on their specific travelers. Does the solution support defining the organizational breakdown structure (OBS) and allow you to select an organizational unit (or level) for reporting and downloading?
5. **Employee Contact Information** – Knowing who may be impacted is good, but quickly identifying how to contact them is even more important. Does the solution capture a range of contact information from sources such as booking and HR data feeds? Does it allow the employee to maintain their own contact information? Does the solution make it easy to go from “who is impacted?” to communicating with them? Does the solution support two-way communication so that you know who got the message and who may need additional help?
6. **Event Situation Reports** – Keeping you and your travelers informed during a crisis is extremely important. The system should automatically send these updates to impacted travelers so that you or your team does not need to spend precious time doing this. Does your TRM vendor provide timely situation updates? Are they easily understandable and accurate? Ask a new vendor specifically how they responded to a major event like the ash cloud. How often did they send out updates? Ask for copies and review them.
7. **Query and Reporting Flexibility** – During a major event, a lot of things are going on and managers are asking a lot of questions about your travelers. The solution should support a robust capability to query and report on the captured data. For example, does the system enable you to select a region (like Europe), a country, a city or even a list of airports? What about a hotel query? Does each of these queries allow you to segment by organizational unit and download the results into a spreadsheet?
8. **Alternate Location Information** – During the ash cloud event, many employees took it upon themselves to jump on trains and rent cars to try to get home. In most cases, organizations spent many hours keeping track of employees or, in many cases, lost touch with them altogether. Does the TRM vendor support alternate ways of getting the location of a traveler? For example, a number for an employee to call in and report their location or the ability to capture e-mail itineraries or support for mobile phone GPS tracking?
9. **Supplier Communications** – While not directly related to the travel risk management or traveler tracking solution itself, a critical part of the process includes the communication of your TRM policy to your travel management company and other key travel suppliers to ensure that there is a clear understanding of your expectations and deliverables in the event of a crisis situation. You need to openly discuss your emergency policy, processes, and procedures with your key travel vendors so that they can assist your travelers in a way that meets your organization’s needs. Your TMC plays a vital role in the efficient technical connectivity between your company and any third-party TRM supplier. Beyond that, the TMC must be prepared to deal with the urgency of a crisis or emergency situation at a time when call volumes may rise dramatically.

From these critical considerations, it can be seen that the success or failure of a TRM or traveler tracking solution largely rests on the data that is fed into the system. This is why the review of the TRM3 Data Management KPAs is so critical when evaluating both your program and

potential vendors. You need to consider all the data that is needed in a crisis – itineraries, traveler contact information, organizational structure, etc.

Pricing Models

While pricing for traveler tracking and risk management products varies from supplier to supplier, there are three basic pricing scenarios. Please note that it is not possible to determine a level, generic pricing field for an organization wishing to implement a traveler tracking tool or a travel risk management solution without a formal RFP that details the specifics of the organization's requirements. If you have a desired pricing model (or billing structure), ask for it. Most of the major suppliers will support a range of pricing and billing options.

Traditional Model

- There is an initial or annual licensing fee charged, with discounts that apply for multiple license subscriptions.
- There is an implementation fee associated with the initial launch of the product, with additional charges that apply for implementing each new data feed based on an agency (pseudo city code) location.
- Tracking is charged by PNR, and there is tiered pricing associated with volume of trips (i.e. PNRs) processed.

Menu Driven Pricing

- There is no general implementation fee; however, there are separate charges incurred depending on the types of services offered and contracted for (i.e. medical assistance).
- Tracking is charged by PNR, and there is tiered pricing associated with the number of PNRs actually used.

Firm Fixed Price Program

- Typically involves sizing the program to the organization on an annual basis resulting in a fixed annual fee as long as the program is within the agreed upon volume ranges.
- There is an initial licensing fee for a fixed number of user logins, with an additional fee charged for each additional user login requested thereafter.
- There is a one-time data feed implementation fee for each pseudo city location issuing travel.
- A base rate is charged for up to a fixed maximum of travelers (or trips), with an additional per transaction fee for each traveler (or trip) that exceeds that limit.

Billing

Each corporation administers traveler tracking supplier charges differently. In many cases, the charge back process is similar to that utilized to charge back travel management company transaction fees. Some possible methods are as follows:

- Organization is billed and charges are paid for centrally by the organization.
- Organization is billed and charges are allocated back to each department on a periodic (usually monthly) basis in accordance with department usage.

- Organization has established coordinated procedures with the travel management company and traveler tracking supplier to add the transaction fee on a point-of-sale basis.

The Business Case

Traveler tracking is the foundation for any travel risk management program; and a comprehensive, technologically sound travel tracking system is essential to meet the duty of care (DOC) standards that are becoming the norm in the modern corporate, academic, governmental, and non-governmental travel realms.

While there is no data available as to how many organizations have already developed and implemented a comprehensive DOC strategy, it has been suggested that organizations do not always seem to provide the right level of care. Even for organizations that have at least started the process, there are gaps in truly securing the well being of their employees. In courts of law around the world, these gaps could be perceived as employer negligence (Advito, 2008). The question that remains to be answered is whether a business case can be made to justify the development of an all-encompassing DOC strategy, with policies, processes, controls, clear lines of responsibility, and tactical implementation built around a system that lets companies know where their people are during any emergency. In economic times of cost containment, such investments will come under intense scrutiny.

A recent case study on implementing a safe business travel policy at a company called Aegis reports that “the potential cost benefit of a global emergency travel and medical insurance policy was investigated and it was concluded that this was cost-effective and useful to introduce” (Beale, 2007). In order to calculate a return on investment for developing and implementing a comprehensive DOC strategy for international assignees and business travelers, an organization will need to carefully analyze its expatriate and business traveler population. First, the types of international assignments (short-term international assignment, long-term expatriation, international business travel, and international commuting) vary in duration and scope. Second, the risks and threats of these assignments vary significantly depending on the home and host locations. Third, the level of risk varies by country. Fourth, the risks also vary by the work responsibilities of the employee based on their job description and the needs of their particular mission. Fifth, employees may have family or significant others accompanying them, changing the range of the employer’s liability. Finally, individual employees have different risk behaviors.

The business case for implementing DOC standards falls in line with the basic tenet of risk management theory: the cost of prevention is cheaper than the cost of dealing with incidents. With regard to travel management, it has been argued (Arnold, 2008) that a proactive approach, including a state-of-the-art travel risk management system, can also translate into efficiency and cost savings by helping avoid additional costs (hotel overnight stays, missed client appointments, unproductive hours spent sitting in airports, etc.) Unfortunately, employers often take a reactive approach, managing risks after incidents have occurred.

The table below details some of the general costs and benefits of employer DOC strategies. In some industries, such as in oil and gas and construction, the number of reportable incidents, which increase without a DOC approach, affects the bonuses of managers. This leads to the organization’s decreased ability to attract customers or investors and may trigger liquidated damages under client contracts. Ultimately, the impact will influence share price.

Cost and Benefit Components	
Cost Components	Benefit Components
<i>Cost of Lack of Duty of Care</i>	<i>Benefit of Duty of Care</i>
Cost of an incident/injury to the victim(s) (i.e. loss of life, emotional distress, lost earnings)	Maintenance of employee well-being (health, safety and security, life)
Cost of medical expenses, treatment, evacuation, and repatriation	Better trained and prepared workforce
Cost of sick pay for employees	Avoidance of costly incidence costs
Cost of diversion of resources (financial and human)	Possibility of greater bonuses for managers and employee profit sharing (if applicable)
Cost of extensive executive resources to deal with the situation	Getting an insurance premium discount if appropriate risk management measures are in place
Property and economic damage	Greater legal compliance
Cost of business interruptions, downtime, closure of a site	Avoidance of litigation
Cost of employment litigation	Increased ability to attract and retain employees
Cost of damages resulting from liability	Increased ability to attract customers/investors
Cost of fines and penalties under relevant laws	Improved CSR reputation
Cost of insurance premiums rising as a result of the incident	Improved productivity
Costs of morale and productivity loss	Increased morale
Cost of loss of potential employees who can't be recruited	Increased reputation and employment brand
Cost of replacing employees who leave (recruitment and on-boarding)	
Potential for bankruptcy	
Cost of the loss of goodwill	
<i>Prevention Costs</i>	
Cost of developing a risk management plan	
Cost of compliance and training	
Cost of insurance coverage	
Cost of vendors	

Finance departments and business managers are well attuned to creating business cases and performing cost-benefit analyses. Finance, HR, Security, Medical, and Management teams should work together to perform a useful analysis of their own risk and DOC obligations. There is both a "stick" and a "carrot" to any travel risk management program. The "stick" is meeting legal compliance and reducing/avoiding negligence and liability. The "carrot" is multi-faceted: employee well being; business continuity; reduced costs (for avoidable expenses like medical care, evacuation, productivity loss); protecting the reputation and brand of the organization for recruitment and retention purposes; and, last but not least, increasing employee well being and productivity by avoiding illness, injury, and possible death.

In any of the emergency scenarios that we might contemplate -- whether they involve medical emergencies, security crises, natural disasters, or other elements -- time is virtually always a factor. Situations normally deteriorate and become more expensive to resolve the longer one delays in responding. Not being able to immediately pinpoint the location of employees affected (or not) by a given emergency is bound to complicate efforts to respond and cost more, in many

ways. The arguments for prevention far outweigh the costs of employee injury or death, and managers who fail to undertake a cost/benefit analysis will (given the size of the potential exposure) be failing in their commercial, fiduciary, and moral responsibilities as managers.

Conclusion

As a direct result of 9/11 -- and a series of major events since then -- systems to mitigate risk and vendors available to assist during difficult times are readily available. The responsibility to select, implement, maintain, monitor, and become a contributor of critical data has fallen into the hands of most corporate travel managers. This document, along with other travel and meetings risk management documents, are available to assist with this enormous responsibility.

NBTA Travel & Meetings Risk Management Committee (June 2010)

Shelly Lewchuk, CCTE, CTE
Committee Chair
Manager, Corporate Travel
Canadian Natural Resources Limited

Bruce McIndoe
Committee Vice Chair
President
iJET Intelligent Risk Systems

Kelly Everhart
Managing Partner
Strategic Management Solutions, L.L.C.

Robert Mintz
Division Manager, Corporate Relations & Global Travel
Rotary International

John Rendeiro
Vice President, Global Security & Intelligence
International SOS Assistance

Peter Savage
Vice President
Passport Health

Ron Wagner
Consultant
Corporate Travel & Risk Management Strategies

Anne Waymire, CCTE
Corporate Travel Manager
Aviva USA