Taking On Travel Risk Management

DESPITE THE INCREASED ATTENTION CORPORATIONS ARE PAYING TO THEIR travelers' safety and security as a globalized economy, geopolitics and instability converge, experts remind companies that safety and security have as much to do with mundane threats as with terrorist attacks. Whether a hurricane, a city center bombing, the flu or exhaustion, work with HR and risk/security departments to have plans in place, to open communication lines with travelers and to keep your travelers educated.

I. GET STARTED

A successful TRM program will include a well-communicated and comprehensive policy, consistent training of new and longer-term employees and support from corporate security.

  A. Develop a vision for the TRM program and set objectives. Consider the role of the TRM program in the company's and travel program's overall goals and decide where TRM should sit within the company's risk management program. Goals could include:
   1. A more comprehensive approach to ensuring travelers' safety and security.
   2. Better understanding of the levels of emergencies, plus creation of response protocols for each.
   3. Increased visibility into travel in higher-risk areas.
   4. Increased ability to track every traveler on the road.
   5. Better communication with travelers during emergencies.
   6. An effective plan to handle travelers' medical emergencies.
   7. Closer compliance with duty of care regulations in the countries to which your company travels.
   8. A comprehensive approach to limiting the risk to the sensitive company data that travelers hold.
  B. Build a network of stakeholders.
   1. Identify a senior executive or manager to champion the program. Doing so will raise the visibility among senior management and lend credibility to the developing program throughout the company.
   2. Coordinate with corporate security, HR, the legal department, the compliance department, corporate communications, IT and frequent global and domestic travelers.
    a. Consider a council of stakeholders, with representatives from each involved department, that meets regularly to discuss and assess developments in the TRM program.
    b. When incorporating travelers into the discussions, ensure that international travelers are represented, including those who are not based in the company's home country. Also ensure that male and female travelers are represented, as well as travelers from all age groups and other demographics.
   3. Consider the role of your travel management companies, online booking tools, TRM suppliers, onsite medical assistance providers and itinerary management technology providers.
  C. Gather data.
   1. Use data sources like corporate cards, expense reports, hotels, airlines, TMCs, third-party data aggregators and internal information to collect data on your organization's travel volume and patterns.
   2. Use the data to see where and how frequently travelers are visiting different locations, including international versus domestic. Learn what countries and regions are frequently visited by your company's travelers and what time of the year and day they typically travel.
   3. Use the data to examine the travel suppliers your travelers use most frequently, particularly when overseas. Document the airlines they fly on, particularly domestic carriers in foreign countries, independent hotels and ground transportation services.
  D. Consider your company's culture and overall goals, as well as the goals of the travel program, when considering the best methods to construct a TRM program. A company that frowns on mandates might resist a TRM program that relies on mandates to govern traveler choice and movement. Some formats to consider:
   1. Mandated policy.
    a. This ensures traveler compliance to preferred booking channels by labeling any deviation a violation of policy and attaching consequences that can run up to nonreimbursement of expenses for repeat offenders.
    b. Some companies require pre-trip approval from the traveler's manager, at the least, before the traveler can book a trip to certain

high-risk locations.

   c. Some companies mandate airlines, hotels and ground transportation providers in high-risk areas or prohibit suppliers with poor safety records.

   d. Some policies require travelers to contact someone in the travel program or at the TMC or to check in from certain destinations upon arrival, at preset intervals during the trip or during emergencies.

   e. As with any policy mandate, expect resistance from some travelers, particularly those who travel frequently to high-risk destinations. Involving them in the development of the program can lower this resistance, as can demonstrating the effect on traveler safety and security that the mandates provide.

  2. Companies with open booking or channel-agnostic travel booking policies can implement technology that records travelers' itineraries before they set off. However, still make every effort to educate travelers of the security risks of booking outside preferred channels.

E. Consider your company's IT and communications system needs. Work with IT to assess whether your company's technology can integrate with any TRM-related tool you're considering, including traveler tracking technology, itinerary management technology and global communications systems.

II. ASSESS TRAVEL RISK

Using the data collected about your company's travel patterns with the help of your TMCs and TRM suppliers and other sources, conduct a travel risk assessment to analyze where attention is most needed.

A. Use proprietary information from TRM suppliers if applicable and public data from the U.S. State Department and other countries' governments to analyze the political situations and potential threats in countries and regions to which your company travels.

B. Types of market threats.

  1. Geopolitical, including ongoing or recent civil unrest, war, recent terror incidents and raised threat levels.

  2. Crime levels, including rates of violent crimes, kidnappings, hate crimes and illegal drug trafficking.

  3. Regulatory issues, including border restrictions, tax codes, workers' rights issues and drug laws.

  4. Criminal codes and cultural extremes. Does the government criminalize homosexuality or curb women's rights?

  5. Infectious disease outbreaks.

  6. Weather or environmental hazards. Are there chronic air quality issues in certain markets or seasonal threats like hurricanes or blizzards?

C. Evaluate no less than the top 20 city pairs for risk.

  1. Consider the likelihood of an incident or emergency in a given market.

  2. Should an incident or event occur, what would the impact be on business travelers, and how much damage would it cause?

  3. Search travel data for known high-risk markets. Find out which business units and travelers frequent these areas. Create baseline risk levels for these trips, as well as specific policies and procedures to govern high-risk travel. Prohibit travel to certain markets, if appropriate.

  4. Search travel data for questionable suppliers or suppliers from countries that the government has sanctioned. See if your travelers are using airlines that are banned from operating in the European Union, for example.

  5. Consider additional regulations or safety measures based on business continuity for the most senior executives.

D. Check out the Global Business Travel Association's Travel Risk Management Maturity Model Self-Assessment Tool.

III. DEVELOP A POLICY

A TRM policy will serve as the backbone for your organization's efforts to ensure traveler safety. While some organizations prefer to maintain separate TRM and travel policies, it is more effective if the policies are united or at least intertwined. Here are some aspects to consider when developing a policy.

A. Booking compliance. The most effective way to locate travelers in emergencies is to require their bookings be made through designated TMCs, online booking tools or other channels. If the company permits booking through an array of channels, require travelers to submit itineraries before departure.

B. Restriction of traveler choice.

  1. Trips to areas designated anything other than low risk should require managerial approval. Consider prohibiting the highest-risk locations. Alert the TMC or configure the booking tool to alert the travel department to any such booking attempts or to reject them.

  2. Prohibit travel that uses suppliers that have questionable safety records, or at least require managerial approval.

C. Ground transportation. Require chauffeured transportation in certain countries, particularly when the traveler has never driven there before or when driving patterns are not similar to those

---

Data & Device Security

Today's corporate data thieves have developed remarkably sophisticated methods of stealing information from unsuspecting business travelers' laptops and mobile devices. Steps to protect data:

I. Preventing device and data theft.

  A. Use devices that have removable hard drives, especially when handling sensitive data.

  B. Spread sensitive information among multiple devices. If multiple employees are traveling, store encrypted data on one device while keeping the encryption key on another.

  C. Enable the ability to remotely wipe sensitive data from devices. Should a device be stolen, this would allow an organization to erase that data as soon as the device connects to the Internet.

  D. Examine the Office of the U.S. Trade Representative's list of countries that don't honor intellectual property laws. Data security in these locations can be more challenging.

II. Preventing other data breaches.

  A. Don't disseminate travel itineraries of those who carry sensitive information beyond those who need to know. Should data thieves target your organization, this will limit their ability to intercept data.

  B. Business travelers with access to sensitive organizational data should use more than two virtual private networks other than the company's VPN. This will hinder thieves who can breach a single VPN over public Wi-Fi.

in the traveler's home country. Additionally, consider requiring chauffeured transportation after long flights to prevent drowsy driving.

D. Limit the number of employees traveling together. Especially for senior management, limit the number of travelers that can be on the same flight to help maintain business continuity in case of a catastrophe.

E. Traveler tracking.

  1. Privacy regulations and reluctance of the traveler likely will foil any attempt to track travelers via smartphone GPS. However, allowing travelers to opt in to such a program could give some visibility.

  2. If traveling to known high-risk countries, consider requiring travelers to forward itineraries to the travel department and to check in at certain points, such as arrival and departure.

F. Require all new employees to read the TRM policy when hired. Review it periodically with longer-term employees.

IV. CREATE A STRUCTURE

Create a TRM program structure that efficiently will ensure safety and security for travelers.

A. Create a central point of contact for the program. Whether that person resides in the travel management, corporate security or risk management department, the person or department will own the program and ensure that its policies and processes are updated and current and will disseminate them widely.

B. Set a contact for round-the-clock emergency traveler assistance who can manage suppliers and support, including extraction. That person could be an internal employee or work for the TMC, TRM provider or other supplier. Continually make sure the mechanism to reach this person is up to date, and repeatedly communicate it to travelers.

C. Define protocols and a communication tree for each of the issues/emergencies a travel could encounter. The point of contact and protocols may differ per situation.

D. Create a cross-functional team that will convene immediately in an emergency or crisis like a natural disaster, terror attack or sudden geopolitical shift. This team would assist travelers by whatever methods necessary.

E. Understand the laws and regulations regarding employers' duty of care responsibility in the countries to which your

company travels, particularly in Europe, where such laws can carry significant consequences for noncompliance. Also consider how duty of care applies to expatriate personnel on long-term assignments and to local employees.

V. MONITOR TRAVEL RISK

The true effectiveness of the TRM program will be tested by the travelers themselves. Making sure they are fully supported must be the company's top goal.

A. Before the trip.

  1. Ensure the traveler is aware of the TRM policy. Include how-tos and contact details on the travel itinerary, on the online booking tool home page, on the company intranet and on other internal channels. Even hang posters in coffee areas, bathrooms and high-traffic areas.

  2. Communicate the risks of the planned trip to the traveler. If risk exceeds the acceptable threshold, implement a trip-specific risk-mitigation plan.

  3. Rehearse the protocols with travelers, particularly for high-risk travel, such as the travel manager reaching out to potentially affected travelers and travelers calling, emailing or texting to check in.

  4. Design role-playing seminars for senior-level travelers and require their attendance. They may be at risk in different ways than the typical business traveler. Work with your TRM provider to create these specific programs.

  5. Ensure the traveler's profile includes every possible point of contact, including mobile phone numbers, email addresses and even social media contacts and Skype addresses.

  6. Ensure the traveler's phone will operate in the destination country or location.

  7. Monitor the situation at the traveler's destination, as conditions may change abruptly. TMCs often offer 24/7 risk monitoring and can automate alerts to travelers who booked through the TMC or approved booking tool.

B. During the trip.

  1. Use mobile alerts and messaging. You can use round-the-clock risk-monitoring tools with SMS alerts to update travelers, and mobile messaging tools can include "help" or "I'm OK" buttons.

  2. Particularly for high-risk markets, GPS tracking can be installed on mobile phones if the traveler opts in.

  3. Explore predictive risk monitoring.

Artificial intelligence tools can digest historical and current data on crime, geopolitics and other factors to predict emerging market-specific threat levels.

C. Should an emergency occur:

  1. Convene the internal cross-functional team.

  2. Contact the TMC and other support to determine if any business travelers are in the location affected. If so, attempt to contact them via a geolocated blast email, SMS message and other mobile messaging tools.

  3. Should a traveler indicate assistance is necessary, contact corporate security and the TMC, business travel insurance provider or TRM supplier to help deploy support, be it finding housing or medical attention or even to arrange extraction.

D. After the trip.

  1. Report any medical emergencies or other incidents through proper channels.

  2. Consider trip stress analysis and notification. New tools can track individual traveler patterns to advise companies and alert employees that their choices may affect their health and productivity.

VI. ANALYZE EFFECTIVENESS

Even organizations with mature, effective TRM programs should strive for continual improvement. Ensure the program is as current and as widely disseminated as possible and measure effectiveness.

A. Implement a training program for travelers and stakeholders to ensure all parties understand the program and know their roles and responsibilities.

B. Implement incident management exercises with key stakeholders. Practice TRM procedures and the escalation process periodically before emergencies turn into crises.

C. Make a record of all incidents and track the performance of the program. Did internal stakeholders and external partners follow response procedure? Was the response time and method effective? Did any affected travelers go unassisted?

D. Implement an improvement plan. Report incidents and performance to executive management. Identify any areas where the process was less effective than planned. What lessons could be learned from each incident?