eBook

everbridge™

Factors to consider before purchasing a travel risk management solution

The most important questions you should be asking

In today’s unpredictable world, organizations need to stay resilient in order to maintain successful operations.

It’s even more important when you are responsible for employees traveling around the world – no matter whether they journey to traditionally ‘safe’ areas or more high-risk destinations.

With the increasing use of Travel Risk Management (TRM) systems, it’s become easier for management teams to quickly understand the scale of their human exposure to high-risk events.

But when considering which system to choose, is that enough?

Although the growing need for these systems may be undisputed, what is not so clear is how much they can vary.

On the surface, they may seem to offer very similar features but, in reality, they can differ greatly in their underlying functionality and capability.

When looking for a system for your organization (or if you’re simply wanting to review what you currently have in place), where should you start?

To help you make an informed decision, here are some of the questions you should be asking about any TRM system and its provider.

Covering off the basics ...

When reviewing the options, there are some basics that you should be automatically asking any provider about the system they are offering:

- Does it instantly identify travelers in an incident-impacted location, those en-route or due to depart in the coming hours, days or weeks?
- Can it automatically distribute travel policies, security briefings and other notifications?
- Can it track key individuals, such as board executives or other VIPs, or number of employees authorized to travel together on any specific flight, train, or vessel?
- Does it monitor pre-, active-, and post-trip travel patterns?
- Does it enable you to react immediately to developing situations and threats?
- Does it enable searches to be performed utilizing a multitude of parameters such as date range, name, flight number, city, hotel name, security status etc.?
- Does it allow searches to be conducted from web-enabled devices such as smartphones and tablets?
- Does it store comprehensive traveler information such as copies of passports and visas, full travel schedules, bookings and tickets, medical and next of kin information?
- Will it automatically compile detailed logs of events and communications that can be interrogated and used to demonstrate that duty of care obligations have been complied with?
- Does it archive all data within the system for an agreed period, providing a fully referenceable audit trail?

As a starting point, these are key features that you would expect any comprehensive TRM system to include. But don't fall foul of the proverbial assumption. Better to ask the basic questions now than be surprised by some unexpected answers later.

The not so obvious ...

If you're happy the system you're considering can at least tick the major boxes, don't be afraid to dig a little deeper. Below you'll find outlined a number of other key questions that should be asked of any potential provider.

1. Is the system truly customizable?

One size certainly does not fit all. Every business is different, so when considering a TRM solution, make sure you find one that's right for you, your organization, and your employees. Talk to the provider about your operating methods, your policies and procedures and your organization's risk strategies. For example:

- Can the system be configured to not just support, but help to enforce, your travel management policies?
- Can it be configured to allow different user permissions to view multiple levels of information?

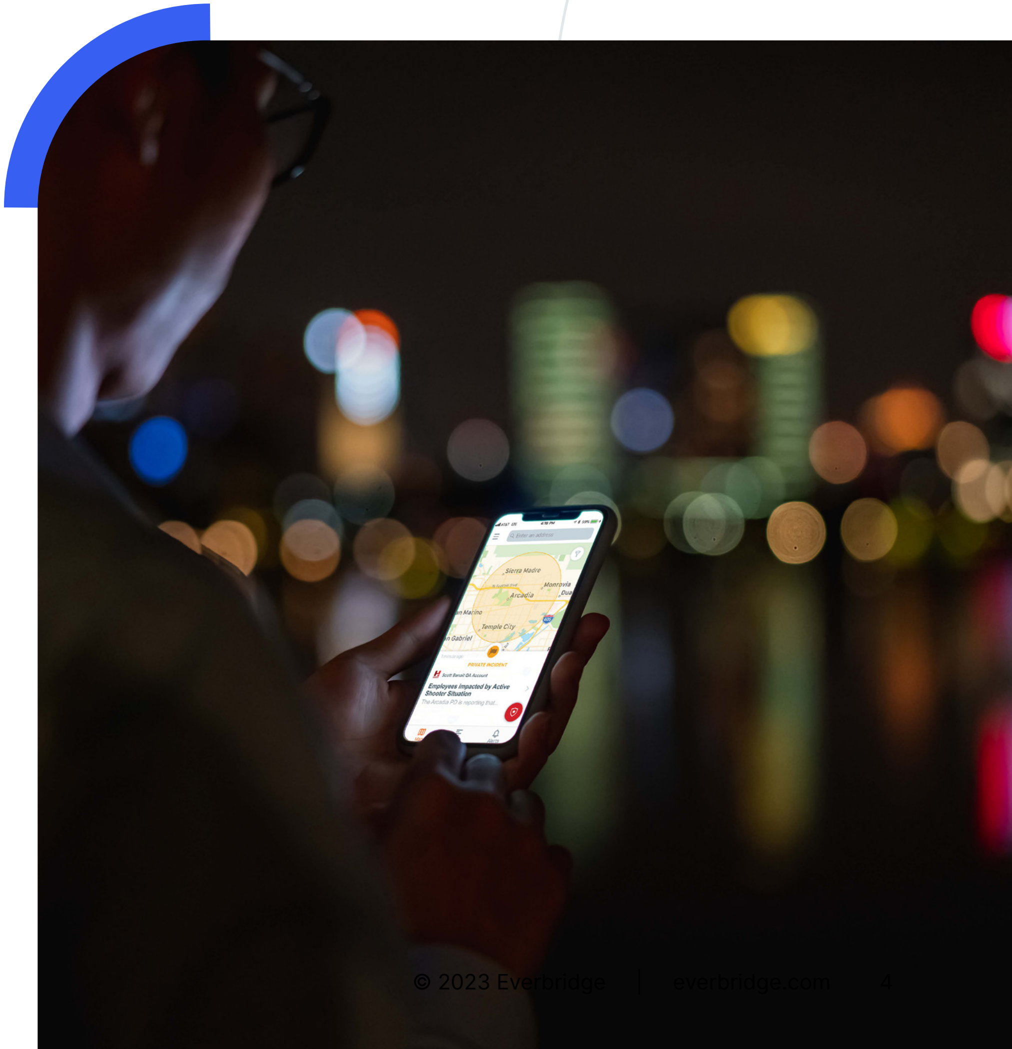
Make sure that the system works with you, not against you. If you feel like you're having to compromise over requirements, it should set alarm bells ringing.

2. Can it cover more than just your travelers?

For simplicity, this guide has referred predominantly to international travelers, but it's important for you to think beyond the needs of just these individuals.

When considering any TRM solution, make sure it also looks after the requirements of others under your duty of care remit, including domicile workers, remote workers, domestic travelers, expatriates and contractors.

A comprehensive solution should be able to cater for the needs of all your personnel, wherever they may be.



3. Does the system operate in real-time?

Although you may assume that all TRM systems operate in real time, this isn't always the case.

Far from providing live information, some systems will be updated with itinerary details at set intervals, sometimes only daily.

The whole nature of risk means, more often than not, that it's anything but predictable and you'll rarely get 24 hours' notice of incidents.

As people's travel plans will also change, you need to carefully consider the implications of choosing a system that could potentially be anything up to a day behind.

4. Is the system developed and maintained in-house by the provider?

Don't be afraid to ask probing questions about the development process.

- Has the system been developed entirely in-house?
- Does the provider outsource parts (or all) of their technical work?

You should be looking for assurances that the system has been (and continues to be) developed by a highly skilled team who can demonstrate a serious commitment to investing in R&D and who can provide exceptional levels of technical support.

There should also be a clear roadmap of future developments, providing assurances that the system is both stable and future proofed.

5. Does it connect directly with the major GDSs?

Does the system connect directly with the major Global Distribution Systems or are aggregators involved in the transfer of PNR (Passenger Named Record) data? Bringing an aggregator into the equation could impact your data supply chain resilience, which you need to be aware of when deciding on your chosen path. By introducing an unnecessary third party (and one with whom you have no direct relationship), control of the data supply chain is lessened and concerns over data privacy and data integrity are heightened.

If you do opt for a provider with direct GDS connections, don't be afraid to ask further ques tions about their GDS relationships. For instance, has the system provider been granted official development licences by the GDS and do they have their full cooperation for future developments? Does their system connect with just some or all of the major GDSs? Even if your current GDS is covered, what if you decide to change?

6. What if you want to operate beyond the typical GDS route?

Although you may want a system that connects directly with the major GDSs, you may also need to consider other options when managing your corporate travel bookings.

Can the tracking system also capture booking data from major airlines, hotel chains, car rental companies, budget operators and popular online booking sites? And can it do this without the traveler or travel booker needing to submit time consuming forms? What limitations does it have?

The nature of business travel is changing, and so are the needs of your travelers. Will the system allow you the choice and flexibility you need to embrace these changes, allowing you to have total visibility of current and future itineraries, regardless of the booking method?

7. Does it rely on you maintaining a relationship with a core TMC?

Does the system rely on your relationship with a particular Travel Management Company (TMC)? Does it allow you to use more than one?

What happens if you decide to change?

If your organization uses different TMCs around the world, make sure the system can connect with all of them and accept data without a conflict in interest.

8. How safe is your data?

Travel Risk Management solutions require robust and accurate information to be available at times of crisis, so understanding how equipped a provider is to deal with cyber/IT security issues should be a key part of the discovery process.

Understanding where and how data is processed, stored, and transferred is critical. Can the provider offer categorical assurances, for instance, that every one of their clients is provided with a dedicated database in order to ensure true data segregation and prevent possible data leakages?

Ask them openly if they have ever suffered a data security breach and, if so, what they did to redress the matter.

Also, talk to providers about their approaches to ensuring data security, data privacy and confidentiality, integrity and availability (CIA) adherence.

Specific questions around CIA should include:

Confidentiality

- Is data encrypted to maintain confidentiality and safety?
- Who else has access to your data?
- What safeguards are in place to protect your data?
- What checks are made on the provider's own staff to ensure trustworthiness?

Integrity

- How are systems designed to maintain the trustworthiness, consistency, and accuracy?
- What prevents data or systems from being tampered with?
- How would the vendor know if data had been tampered with?

Availability

Recent history shows countless examples of major IT breaches and security failures that caused serious issues. While some incidents are inevitable, it is important to ensure that your provider has taken

all the necessary precautions to mitigate against potential risks. Ask them the following:

- Is data replicated between different data centers?
- Is data stored within Redundant Arrays of Independent Disks (RAID)?
- Are High Availability (HA) clusters used to provide continuous uptime?
- What methods are in place to mitigate denial-of- service?
- What disaster recovery procedures are in place?

In short, can they provide you with data supply chain custody that you can be truly confident in?

9. Are you staying on the right side of the law?

GDPR – Is the provider compliant?

Ask about General Data Protection Regulation (GDPR) compliance. The GDPR is a regulation that replaced the Data Protection Act 1998 and has been in force since 2018.

Any company (regardless of their own physical location) that processes the data of EU citizens needs to comply, so make sure that the provider you deal with is fully informed and ready. Ask what processes they have in place to ensure compliance. As the ultimate data owner, you could find yourself liable for any breaches on their part.

Data residency – Are you compliant?

Parallel to the GDPR considerations, it’s also essential to understand exactly where your data will be stored by your chosen provider. Data laws and regulations can differ greatly from country to country.

10. Are dots on a map enough?

You may have been reassured by the supplier that their solution ticks all the boxes from a technical perspective, but before you make a final decision, step back and remind yourself of your key objective.

Demonstrating adequate duty of care goes much further than simply being able to locate your people on a map and respond to an incident.

Understanding the risks you are exposing your travelers to, assessing those risks, and having the necessary risk mitigation measures in place is paramount.

Without this, or being able to demonstrate how this was considered, you'll be falling a long way short of fulfilling your fundamental duty of care requirements. Having dots on a map is one thing, but truly understanding how they got there is even more important.

Ask yourself the following:

- Do you have a clear and accurate real-time picture of the risks and the dynamic threats your people face?
- Do you have the right policies and procedures in place to contextualize, understand, and treat these risks?
- Are the policies and procedures engrained across the whole organization? Are they documented, understood, and complied with?
- Before a trip is even booked, is a comprehensive risk assessment carried out and are adequate control measures in place?
- Are your travelers provided with the necessary briefings and training to prepare them for all circumstances before they travel?

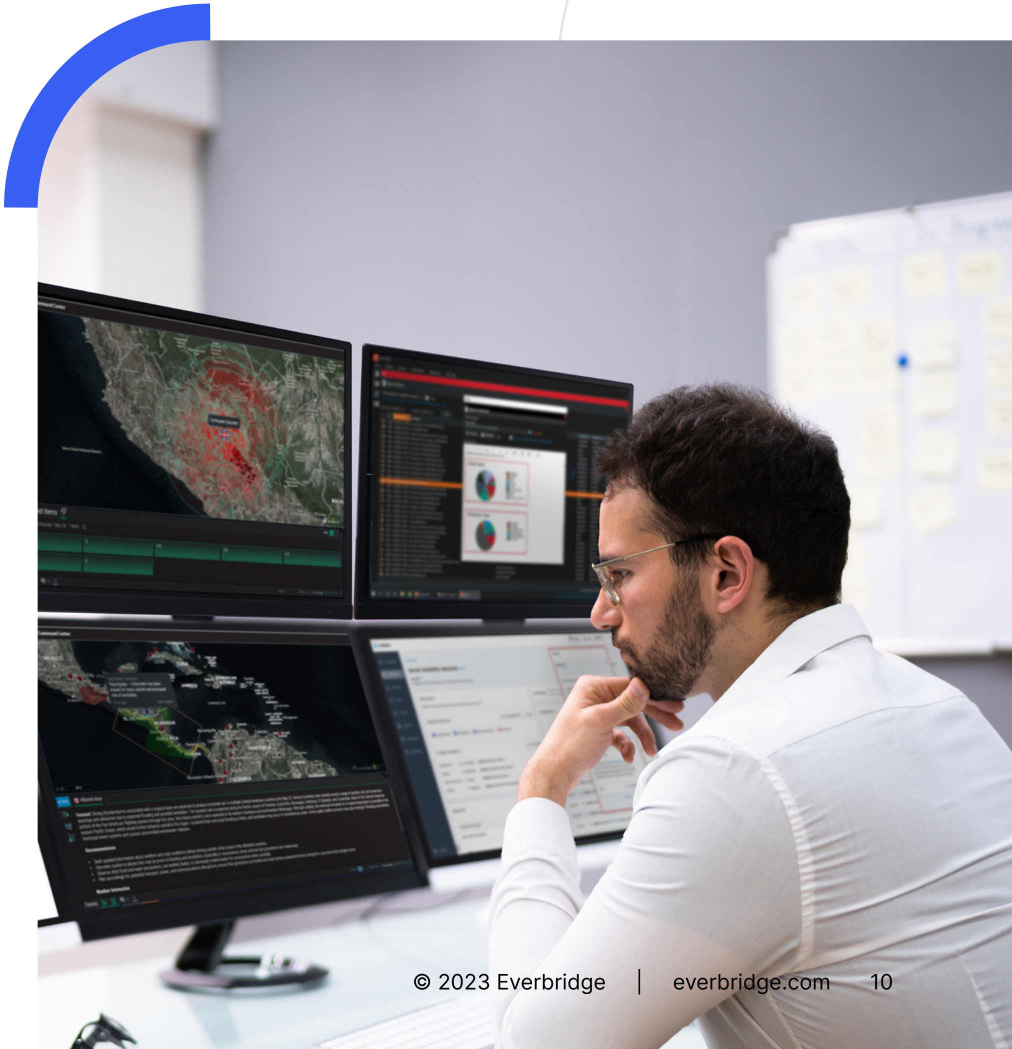
When incidents occur, or are likely to occur, being able to account for your people and provide the necessary assistance is very important. But understanding and being able to mitigate against risk in the first place is an essential, yet often overlooked component of any truly effective risk management framework.

11. Can you integrate with a broader Critical Event Management (CEM) platform?

At this stage, you may be focusing your search on a system that can simply track your travelers, deliver real-time intelligence on their locations, and alert them (and you) to potential risks.

Beyond that, it's important to also consider other requirements that you may have in the future and whether the same provider will be able to fulfill these in-house.

Ask the provider if they offer a single unified CEM platform that will allow you to manage the full lifecycle of a critical event. Is it able to offer integrated solutions across the five core resilience areas: Business Operations, Digital Operations, People Resilience, Public Safety, and Smart Security? Can it quickly and reliably aggregate and assess threat data, locate people at risk, and automate the execution of pre-defined communications processes? Can the provider also provide on-the- ground in-country medical and security assistance services 24/7, providing an immediate response for your people, no matter the issue?



© 2023 Everbridge

In summary

You'll undoubtedly have your own priorities and your own set of questions when evaluating any potential system and provider. In order to find the solution and provider best suited to your organization, don't settle for the standard sales pitch and don't be afraid to ask some probing questions. A good provider will welcome questions, and will happily take the time to provide comprehensive and honest answers.

Finding answers to these important questions will prove more than worthwhile when you find the Travel Risk Management system that truly works for you, your travelers, and your organization.

everbridge™

About Everbridge

Everbridge, Inc. (NASDAQ: EVBG) empowers enterprises and government organizations to anticipate, mitigate, respond to, and recover stronger from critical events. In today's unpredictable world, resilient organizations minimize impact to people and operations, absorb stress, and return to productivity faster when deploying critical event management (CEM) technology. Everbridge digitizes organizational resilience by combining intelligent automation with the industry's most comprehensive risk data to Keep People Safe and Organizations Running™.

For more information, visit Everbridge.com, read the company blog, and follow us on LinkedIn and Twitter.

Get in touch to learn about Everbridge, empowering resilience.

everbridge™