

Phil Barone

Vice President Global Guardian



- 17 year Assistance Veteran
- Human Capital and Asset Risk Mitigation Specialist
- Crisis Management and Duty of Care Advisor

A photograph of the Houston skyline, featuring several prominent skyscrapers like the Bank of America Tower and the JP Morgan Chase Tower. In the foreground, there is a river with a bridge and some greenery. The image has a semi-transparent overlay.

4 Dimensions of Travel Risk Management

THE HOSPITALITY LAW CONFERENCE: SERIES 2.0 - HOUSTON

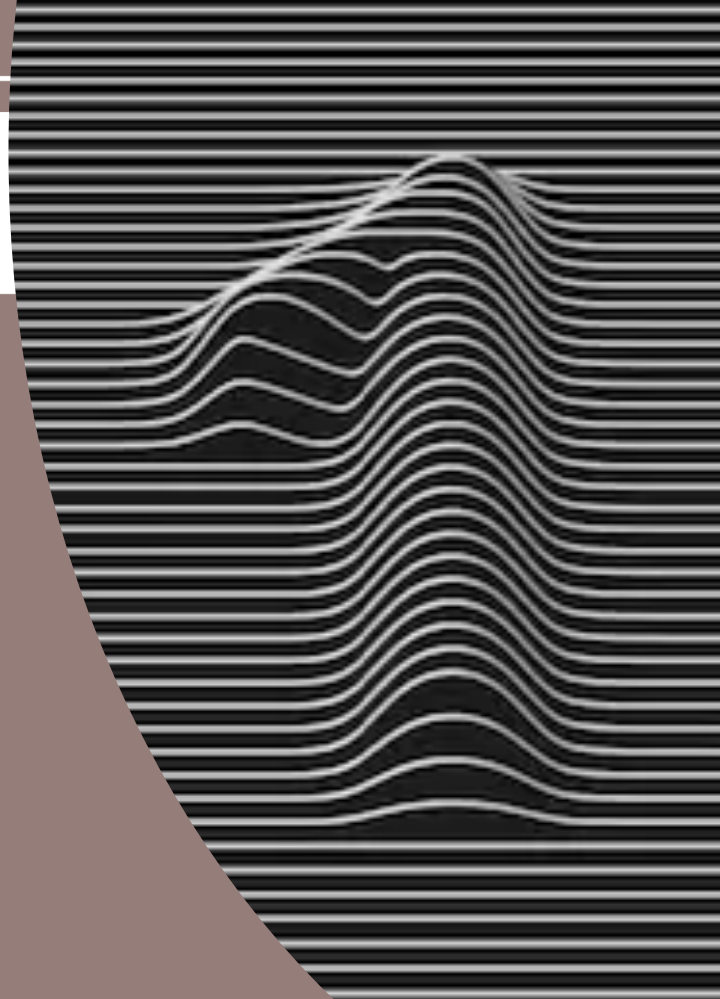
APRIL 9 - 10, 2019

What is TRM?

- Travel Risk Management is a comprehensive, consistent and proactive approach to protecting your people and your organization from travel risks



1st Dimension



9-11

- No Technology to Account for Travelers
- Domestic Terrorism
- Domestic Employee Support
- Travel Risk Management non-existing
- Assistance Industry Focused on Reactive Response
- Invention of Travel Tracking



2nd Dimension



Pandemics

- Policy development across functions
- Committee lacked experience to build pandemic plans
- Implementation hugely complex
- Procurement of PPE and Tamiflu distribution
- WHO stage changes and actioning by region or country
- Local National, Expatriate, International Traveler considerations
- Ingress and Egress of facilities
- 2007 UK Corporate Manslaughter Act



3rd Dimension



Terrorism

- Arab Spring “broke” all plans
- Management of simultaneous events
- Lack of “employee preparation”
- Corporate policy and Communication flawed
- Lack of large scale evacuation planning
- Media and intelligence called it “late”



Volcanic Ash Cloud

- How do you prepare for this????
- No policy in place to get them home
- Stranded employees ran out of money and medicine
- Travel accountability “Where are they”
- Corporate travel companies overwhelmed
- Security at Airports and Train Stations to keep the mob at bay
- Companies and airlines at mercy of UK Civil Aviation Authority



4th Dimension



Digital Terrorism

- Cyber attacks
- Cyber Ransom
- Cyber Terrorism
- Lockton Report 80% companies hacked
- Technology stove-piped
- Internal business functions lack of coordination
- Insurance policies in their infancy
- Cyber vendors not “responders”
- FBI overwhelmed with requests
- Hackers will “shut you down” and take your money



We've been Hacked ... now what?

- Senior leadership Involvement and alignment is essential (CEO/General Counsel/CISO/IT)
- But that's not enough
- Hundreds of vendors and products
- No true “blueprint” of your digital infrastructure.
- “Most” have not contracted with an Incident response vendor who can align all functions, advise leadership and negotiate with hackers



Future of Travel Risk Management

- Assume it will happen to you
- Start at the top (General Counsel)
- Invest, test and train
- Cross function collaboration is key
- Find a 4 dimensional vendor that possesses the “SO WHAT” factor
- Protect your People, Assets and Communications.....Your reputation depends on it.

