Flying by the Seat of their Pants

An Examination of Contemporary Travel Security Risk Management

Submitted by

Gian-Rico Luzzi

Student No: [redacted]

Submitted in partial fulfilment of the requirements of the award of Master of Science in Security Management

Loughborough University Masters Project

Module Code: 13BSP558

Word Count: 21922

28 November 2014

CERTIFICATE OF ORIGINALITY

This is to certify that I am responsible for the work submitted in this report, that the original work is my own except as specified in acknowledgements, footnotes or in references, and that neither the dissertation nor the original work contained herein has been submitted to this or any other institution for the award of a degree or for any other purpose.

Abstract

Business travel is a fact of life for many organisations. This practice, which is being utilised more and more as businesses expand operations and services due to globalisation, exposes a business and its travellers to significant risk. Due to the ever increasing scrutiny of failures by the media, legal entities and the government, the researcher embarked on the project to determine how developed the travel security risk management practice used by contemporary businesses is in terms of maturity.

A gap in the literature was discovered whilst conducting the literature review as much of the literature on the subject is related primarily to the topics of duty of care or corporate social responsibility. Quantitative data collection involved surveying recognised business leaders, security and human resource professionals. Qualitative data collection involved interviewing representatives from large multi-national organisations responsible for the function.

Cross verification of results using triangulation identified that the travel security risk management practice used by contemporary businesses is generally immature and the topic is still in the early stages of development. The research recommends that the practice be addressed strategically with a person accountable assigned, preferably from a security department, designing and implementing a pro-active and robust travel security risk management programme which encompasses several compulsory components.

The research also highlights the immediate market need for a business travel security standard, in order to develop the generally informal, ad hoc and somewhat reactive practice many organisations are currently adopting, and developing this to being a more formal, structured and pro-active risk management practice.

Acknowledgements

There are a number of people who I would like to thank for helping me down this road of discovery during the last three and a half years. Most importantly my wife, [redacted]. Thank you for your unwavering faith. It has helped more than you will ever know, not to mention the sacrifices that you have made to allow me to achieve my goal. [redacted] and [redacted], my amazing children. You have been my inspiration, and I can only hope that this will in turn inspire you one day.

To my mother, thank you for your support, and many hours of proof reading. To my brother [redacted] and my dear friend [redacted], thank you for your continuous encouragement. To my friends, thank you for your support and understanding. I am looking forward to having some free time to spend with you again!

[redacted] and [redacted] thank you for making this all possible. [redacted], [redacted], [redacted], [redacted] and [redacted], thank you for your time and effort in assisting me. [redacted] my supervisor, thank you for your empathy during difficult times and for being my guide.

Thank you to all the business leaders, human resource and security practitioners who took the time to participate in my questionnaire, and those that facilitated the access. To the three representatives who granted me interviews, I thank you for your time and effort, but most importantly for your trust.

Last but not least, my thanks go to my late father who taught me how to be hard-working. Without that I would never have survived this journey. I dedicate this work in loving memory of you.

Table of Contents

		Page
Table of Contents		iii
List of Appendices		iv
List of Figures		v
List of Tables		vii
List of Abbreviations		viii
Chapter 1	**Introduction**	1
Chapter 2	**Literature Review**	6
	Stakeholders	8
	Risk Management	13
	Risk Assessment	17
	Promulgation	18
	Risk Treatment	21
	Evaluation	27
Chapter 3	**Research Methodology**	31
	Literature Review	33

		Page
	Survey	33
	Interviews	40
Chapter 4	**Research Findings**	44
	Stakeholders	45
	Risk Assessment	62
	Promulgation	68
	Risk Treatment	77
	Evaluation	92
Chapter 5	**Conclusions and Recommendations**	98
	Bibliography	105

Appendices

Appendix 1.	Advito High Risk Area Advice	118
Appendix 2.	Online Questionnaire	119
Appendix 3.	Questionnaire Formal Request for Assistance	145
Appendix 4.	Supplementary Questionnaire Formal Request for Assistance	147
Appendix 5.	Questionnaire Introduction	148
Appendix 6.	Interview Request	149
Appendix 7.	Interview Template	151
Appendix 8.	Transcription Interview One	154

Page

Appendix 9. Transcription Interview Two 168

Appendix 10. Transcription Interview Three 179

Figures

Figure 1. BS ISO 31100:2011 Risk Management Process 14

Figure 2. Addressing the Potential Weaknesses of Online Surveys 35

Figure 3. Questionnaire Response – Respondent Job Title 44

Figure 4. Questionnaire Response – Responsibility for Management 46

Figure 5. Questionnaire Response – Departmental Responsibility for Policy 47

Figure 6. Questionnaire Response – Preferred Departmental Responsibility for Policy 49

Figure 7. Questionnaire Response – Departmental Risk Owner 51

Figure 8. Questionnaire Response – Departmental Availability 53

Figure 9. Questionnaire Response – Departmental Responsibility for Pre-Trip Authorisation 56

Figure 10. Questionnaire Response – Preferred Departmental Responsibility for Pre-Trip Authorisation 58

Figure 11. Questionnaire Response – Incident Management 60

Figure 12. Questionnaire Response – Risk Assessment 63

Figure 13. Questionnaire Response – Risk Levels 64

Figure 14. Questionnaire Response – Risk Assessment Information Sources 66

Figure 15. Questionnaire Response – Formal Travel Security Policy 69

Page

Figure 16.	Questionnaire Response – Inclusion in Associated Policies	70
Figure 17.	Questionnaire Response – Pre-Trip Advisory/briefing	72
Figure 18.	Questionnaire Response – Specialised Security Training	75
Figure 19.	Questionnaire Response – Responsibility for Training	76
Figure 20.	Questionnaire Response – Compulsory Pre-Trip Authorisation Procedure	78
Figure 21.	Questionnaire Response – Dedicated Emergency Contact Point	81
Figure 22.	Questionnaire Response – Responsibility for Emergency Contact Point	82
Figure 23.	Questionnaire Response – Active Traveller Tracking	83
Figure 24.	Questionnaire Response – Responsibility for Traveller Tracking	84
Figure 25.	Questionnaire Response – Traveller Tracking Comparison	85
Figure 26.	Questionnaire Response – Traveller Tracking Methods	85
Figure 27.	Questionnaire Response – Security Updates	88
Figure 28.	Questionnaire Response – Responsibility for Traveller Security Updates	89
Figure 29.	Questionnaire Response – Provision of Security Updates	89
Figure 30.	Questionnaire Response – Evaluation Procedures	93
Figure 31.	Questionnaire Response – Initial Respondent Rating	96
Figure 32.	Questionnaire Response – Supplementary Respondent Rating	96

Page

Tables

Table 1.	Stakeholder Awareness levels	10
Table 2.	Stages of Evolution within Travel Risk Management Strategy	29
Table 3.	Features of Qualitative and Quantitative Research	32
Table 4.	Online Questionnaire Distribution	36
Table 5.	Respondent Functional Group Profile	50
Table 6.	Current and Preferred Departmental Risk Ownership	54

Abbreviations

ALARP	As Low as Reasonably Practicable
AMEX	American Express
BA	British Airways
BTSRM	Business Travel Security Risk Management
CONDO	Contractors on Deployed Operations Training
CRG	Control Risks Group
EP	Executive Protection
ERM	Enterprise Risk Management
ESRM	Enterprise Security Risk Management
EXEC	Executive
HEAT	Hostile Environment Awareness Training
INTEL	Intelligence
K&R	Kidnap and Ransom
KPI	Key Performance Indicator
LAT-AM	Latin America
MEDIVAC	Medical Evacuation
MH370	Malaysian Airlines Flight Number Three Seven Zero
MTA	Main Travel Agent
P1	Interviewee One
P2	Interviewee Two
P3	Interviewee Three
PA	Personal Assistant
RL	Researcher
TMC	Travel Management Company
TRM	Travel Risk Management
UK	United Kingdom
USA	United States of America

Chapter 1

Introduction

Business travel is defined simply by Aguilera (2008, p.1109) as '*work-related travel to an irregular place of work*'. The unfamiliarity involved in travelling to a new or rarely visited location is inherently risky and for a business utilizing this practice travel risk management (TRM), as part of the businesses overall risk management strategy, should be seen as paramount.

In the modern day workplace highly influenced by globalisation and expansion, there are numerous strategic and/or operational reasons why personnel have to travel for business. So much so it has become very common for employees to travel as part of their job. United Kingdom (UK) residents for example conducted 6.825 million trips abroad for business in 2013 (Office for National Statistics 2014). This can range from a company director attending a board meeting to security operatives deploying to a war torn area to provide a protective service.

There are several factors driving contemporary TRM. These include organisations ensuring that they are complying with duty of care principles, avoiding criminal liability, ensuring business continuity, preventing reputational damage and demonstrating positive corporate social responsibly. More specifically there are several types of risk related to business travel. These include: risk to personnel, risk to reputation, risk to data/equipment, legal risk, financial risk, and risk to productivity/trip effectiveness (Advito 2009). The most important of these risks being the health, safety and security risks to personnel.

In the UK the Health and Safety at Work Act 1974 and The Management of Health and Safety at Work Regulations 1999 sets out an employer's responsibility toward the duty of care of its staff. This is to ensure the health safety and welfare of their employees

whilst they are at work (Health and Safety Executive 2013). Claus (2011a) highlights that in the context of business TRM this relates to business travellers, locals, expatriates, international assignees and their dependants. In the United Kingdom failures linked to the management of risks resulting in a death are now prosecuted under the Corporate Manslaughter and Corporate Homicide Act 2007 (Health and Safety Executive 2013).

Business travel security risk management (BTSRM) as part of a wider TRM programme is essential to ensure business resilience in contemporary times where political instability, terrorism, pandemics, natural disasters and crime are all too common. Weir (n.d cited in Davidson 2009, p.2) suggests that the goal of business risk management is to, "*make calculated decisions daily to help manage risk to people, reputation, information, and property – in that order*".

Travel risk management is not a new practice, however its profile has increased in recent years. This being caused by the changes in the risks businesses are exposing themselves to, such as terrorism, kidnapping, natural disasters, civil unrest and crime, due to expansion into emerging markets, socio-economic volatility, hostile environments, and the scrutiny of the modern media.

The modern concept of risk management is now widely recognised as an academic discipline. It is widely used by organisations of different sizes and in different industries. '*Whilst it acknowledges that nothing in life is certain, the modern practice of risk management is a systematic and comprehensive approach, drawing on transferrable tools and techniques*' (Hopkin 2010, xxiii).

Organisations now have a host of countermeasures at their disposal to assist in the protective process. Travel security is defined as, "*protective measures for the safekeeping of people, property, and information while temporarily based, or in transit outside their normal area of operations*" (Talbot & Jakeman 2009, p.335). Be it for a business meeting, short or long term assignment, the fundamental problem when

travelling to, and working in, an unfamiliar location is that it gives rise to uncertainty and change.

The way in which we perceive travel security risk is important as the subjectivity involved in risk perception can call into question the severity of a risk which in turn can affect the extent to which the risk is managed. For example with incidents such as the terrorist attacks in New York (USA) in 2001, Bali (Indonesia) in 2002, Mumbai (India) in 2008, In Amenas (Algeria) in 2013 and with civil unrest in many other countries it would seem that travelling the world is getting more dangerous, however crime levels are reportedly falling in many countries each year. In terms of travel security, risk perception may be a helpful driver towards risk management, however the risk must be objectively assessed and evaluated in order to understand what level of risk can be tolerated.

Risk tolerance is defined as an '*organization's or stakeholder's readiness to bear the risk after risk treatment in order to achieve its objectives*' (British Standards Institute 2011, p.9). For example a close protection operative deploying to a high risk location on assignment will have a higher risk tolerance than a company executive travelling to Switzerland for a board meeting, however both still need the risk to be treated to an acceptable level. Achieving this level involves the application of the 'as low as reasonably practicable' (ALARP) principle. (Health and Safety Executive 2014).

In the UK this is a guide, derived from legislation, to determine what a tolerable and acceptable level is. This requires an organisation to weigh a risk against the trouble, time and money needed to control it (Health and Safety Executive 2014). To calculate this an organisation will need to analyse the risk in the context of the organisation as well as the risk management procedure in place and the required controls. However in the absence of a specific travel security benchmark or standard, this leaves only the interpretation of 'reasonably practicable' as a guide when producing a cost benefit analysis, and deciding which preventative and protective controls are commensurate with the risks.

After discussions with security industry practitioners on the topic of travel security it seemed quite open to debate as to whether security issues facing business travellers had become much more prevalent over the last decade, possibly as they may be perceived as 'soft targets', or if it is just the significant increase in use of the practice that has brought so many reported failures to the fore. Mostyn (cited in Cousins 2010) suggests that it is a combination of both as there is now a greater frequency of business travel, and that it is widely known that most business travellers are thinking more about the meeting they are heading to or how may emails they are receiving rather than their security. Cousins (2010, p.29) concurs suggesting, '*Most of us drift through the practicalities of our business trips on autopilot, focused on the job in hand*.

Another consideration is also whether or not serious incidents, such as the aforementioned terrorist attacks, have essentially caused business travellers and/or their organisations to now have a lower risk tolerance level. Fischhoff et al (2004 cited in Ball & Machin 2006) highlight that, '*an individual's willingness to travel to a foreign destination is influenced by whether their estimate of the risk was above or below their general threshold for the acceptability of travel risks*'. What the debate does demonstrate is that contemporary corporate security practices do require considerable focus. Lippert et al (2013) and Walby & Lippert (2014) concur suggesting that there is currently little focus amongst scholars into corporate security despite the increasing prevalence and size of corporate entities.

The aim of this research project is to examine the management of the security risks associated with business travel in order to determine how developed the practice is. In this dissertation the literature review, contained in chapter two, will provide an overview of the stakeholders involved in the practice. It will examine the ways in which this risk is being assessed, the ways in which organisations are promulgating the risks to business travellers and stakeholders, the methods being used to manage the risk and how BTSRM programmes are being evaluated.

Chapter three outlines the research methodology used for the project, which entails using an inductive approach. Data collection for the project will utilise a mixed methods approach. An online questionnaire, disseminated to practitioners operating in a wide range of business sectors through several institutes and organisations, will obtain quantitative data on the topic. These being: The Security Institute; ASIS Europe UK Chapter 208; International Professional Security Association; Association of University Chief Security Officers; Security Risk Management Training Institute; HR Society; Institute of Leadership and Management. Semi-structured face-to-face interviews, with three industry professionals responsible for the function representing large multi-national organisations, will provide qualitative data on the topic.

Chapter four presents the results of the research and using triangulation evaluates these in relation to the findings of the literature review. Chapter five draws conclusions on how contemporary businesses are managing travel associated risk , in order to bring to the fore the state of current practice, develop a benchmark, as well as to provide recommendations on how to improve and develop the maturity of the practice.

Chapter 2

Literature Review

The fundamental component of this research is risk. An understanding of the nature of risk and its management is critical to ensure efficacy of any related programmes or activities. A practical definition of risk to use is that, *'Risk can be defined as the combination of the probability of an event and its consequences.*' (ISO/IEC Guide 73 cited in AIRMIC, ALARM & IRM, 2002, p.2).

In assessing probability it can be seen that a risk can be perceived in a number of different ways. According to Borodzicz (2005, p.46) much risk perception study appears to suggest some '*recurring social features*'. This relates to the way unknown risks are perceived as more frightening than normal every day risks, the fact that voluntary risk is preferred to imposed risk and that the core component of risk, probability, is not easily understood or believed.

It is important for the correct perception of a risk that it is evaluated in a probabilistic context, and not just by focusing solely on the consequences, as the perception of the risk will influence the management of the risk. In relation to business travel risk much attention is now paid to the serious risks such as incidents of terrorism (which now make almost daily appearances in the media), however less attention is paid to the more prevalent incidents of pickpocketing and robbery.

Propensity for risk is another consideration to take into account. This will apply to the business traveller and the organisation. They both may be risk adverse when considering risks affecting health, safety and security aspects, but risk seeking in respect of their financial strategy. What is important here though is the concept of risk exposure. The individual and organisation must be sure that the risk they think they are exposing themselves to, is indeed the risk that is being exposed, and that they do want to be

exposed to it. The only way for this to be effectively done is through thorough risk exposure assessment as part of risk management in order to allow for an evaluation of the responses that are available, and to ascertain which of those responses would best suit the individual and organisation in context. According to Talbot & Jakeman (2009) exposure assessment is a critical activity which is similar to risk identification, but a separate assessment element, which informs all phases of the risk management process.

Security risk management, such as the focus of this research, is a core component and subset of risk management encompassing the security related risks and concerns. It differs to the more generic risk management framework model such as British Standard 31100:2011. Brooks (2011) highlights this is due to the fact that more generic risk management models focus more on probability and consequences and do not consider security concepts such as threat, vulnerability and criticality in uncertain and changing environments requiring specialist security knowledge. The operational management of risk in relation to business travel is analogous to security risk management as it encompasses a wide range of threats, vulnerabilities and hazards. These being terrorism, kidnapping, civil unrest, violence and crime.

When conducting initial searches for literature on the topic there seemed to be a plethora of work published in relation to travel risk management. Upon examination it was discovered that primary sources usually examine business travel risk in several contexts: Risk Management (Advito 2009; Jonas 2012; Mcindoe 2011; Rendeiro 2013; McNulty 2013); Duty of Care (Claus 2011a; Claus 2011b ; Rendeiro 2012; Glab 2012); Corporate Social Responsibility (Douglas and Lubbe 2010; Advito 2007; Beaverstock et al. 2009; Aguilera 2008).

Of these there were three particularly valuable sources of information. The first two being Duty of Care and Travel Risk Management Global and European Benchmarking Studies by Dr Lisbeth Claus of Willamette University in Salem, Oregon, USA. These comprehensive studies used information from 628 global companies. They were published in 2011 by International SOS, a multi-national healthcare, medical and security services company. The third a White Paper published in 2009 by Advito, a multi-national travel management consulting company based in the USA.

Claus (2011a) highlights that contextual influences such as the type of industry and the location in which an organisation operates or involves travel to may influence the way in which the business perceives risk and the internal level of awareness. For example energy and natural resource organisations, and non-governmental organisations operating in hostile and/or environmentally challenging regions are faced with more extreme or unknown risks which are perceived as more dangerous, whereas a multi-store retail business operating in metropolitan suburbs may underestimate the level of risk they are exposed to, as seen in the recent terrorist attack on the Westgate shopping mall in Kenya in September 2013.

Guidelines from Advito (2009) highlight that there may be various stakeholders responsible for the initiation, implementation, ownership and management of a business travel risk management programme. These being dependent on the structure and culture of an organisation.

Stakeholders

Using these guidelines a travel risk management programme requires four key stakeholders: an initiator (a person, department or stakeholder) who highlights the need for the programme; a sponsor (senior management) who will implement the programme and ensure its continuation; a person accountable (usually the person responsible for all risk) for the programme; an owner of the programme who will form, drive and manage a steering group comprising representatives from key departments: travel management, security, human resources, legal and medical.

Advito (2009) includes several case studies which highlight the various manners in which three organisations approach TRM in terms of stakeholders. The first study of The Capital Group of Companies, a multinational investment organisation, highlights that the travel department takes responsibility for travel risk as part of the travel management program, liaising closely with risk management, business continuity, human resources, and compensation and benefits units in a travel risk sub-committee. This sub-committee contracts a travel management company (TMC) to provide tracking and intelligence services and also security expertise due to the absence of an ‘in-house’ security department.

The second study of ING, a Dutch multinational banking and financial services corporation, identifies the corporate security department based at the business global headquarters as being responsible for TRM, contracting the services of numerous TMC's in different locations. This approach however is reportedly in the process of being changed to reduce the amount of TMC's operating to a small number, and coordinating TRM with human resource (HR) and health and safety departments.

The third case study of DuPont, an American chemical company, identifies the global security team as being responsible for TRM, working closely with travel management, medical, crisis and information security teams. Travel is managed globally by a TMC providing full time security reporting. If a situation requiring attention develops, the local or regional security team works together with the travel management team and TMC to locate and assist personnel.

Apart from an organisation's location or operating location and industry, another important aspect, as corroborated by Claus (2011a), is the contextual importance of business size on TRM. Business size for example might cause a variation in stakeholder and department involvement as small or medium sized businesses might not have the dedicated business units that a large organisation has.

Claus (2011a) also suggests that levels of risk awareness are generally greater in larger organisations due to the fact that there are many more employees operating in numerous locations, typically much more mobile encountering severe and diverse risks. Her study findings (Table 1) indicate that levels of stakeholder awareness in terms of their duty of care responsibility varies considerably.

Table 1. Stakeholder Awareness Levels

Stakeholder	**Mean**
Security/Risk Management	4.00
Occupational Health and Safety	3.95
Senior Management	3.56
Operations	3.51
Public Relations/Communication	3.46
Project Management	3.37

Source: adapted from Claus (2011a, p. 24)

From these findings it can be seen that security and risk management score the highest in relation to their level of awareness. In text Claus highlights that human resource departments score just slightly higher than senior management. However most notably senior management only have a medium level of awareness. This is a problem as Claus (2011a) suggests that the two critical success factors to a strategy is ownership and awareness, and it is usually senior management who are responsible for the implementation and resourcing of a travel risk management programme.

Claus (2011a, p. 26) highlights results showing that ownership of the function is divided into three types. These being primary responsibility, coordination, and decision making, and that for each of these the same five departments are identified but in varying orders.

Who has primary responsibility? HR, security, senior management, travel and risk management.

Who coordinates the activities? HR, security, travel and risk management, and senior management.

Who makes decisions in the organisation? Senior management, HR, security, risk management and travel.

Respondents were then asked who they think should own the function. Human resources and security departments (with security ranked behind human resources) were most commonly listed as single owners, however most respondents indicated that it should be shared between departments. Claus infers that this result is "*somewhat surprising*" when results of her study showed human resource departments have low risk perception levels in terms of threats, and low level ratings in terms of duty of care awareness.

In a study comparing the European results of the global study (Claus 2011b), the results are different, in that in the European region, primary and coordination responsibility lies more with security departments, followed by senior management, and that in Europe, human resources, travel and risk management are less frequently identified as owners. In both the global and European studies senior management are shown to lead decision making whilst it is considered it should be everyone's responsibility.

More recent studies and surveys have identified that employee perception of who is primarily responsible, or the owner, of travel risk management varies widely between departments. The Inform Logistics Poll (2012 cited in McNulty 2013) highlights that respondents identified the following departments being responsible for risk management: 35% travel; 30% security; 18% human resources; 9% outsourced. An AirPlus International Survey (n.d cited in Jonas 2012) highlights similar disparity. Respondents when asked which department was primarily responsible for creating policy and overseeing traveller safety and security identified: 20% security; 19% travel management team; 7% human resources; 10% other; 42% a combination.

What is evident from analysis of these studies is that risk management incorporating business travel and duty of care varies a great deal between businesses. This was highlighted during a recent travel management conference in New York, USA, '*It's a little worrying because people aren't always sure who is in charge of risk management within corporations*' (Flint 2013 cited in McNulty 2013).

An important strategic consideration in terms of stakeholders is the phenomenon of groupthink. This group heuristic was identified by Irving L. Janis, a research psychologist at Yale University, USA and defined as, '*a mode of thinking that people engage in when they are deeply involved in a cohesive group, where the members' strivings for unanimity override their motivation to realistically appraise alternative courses of action'* (Rahim 2011, p.132).

In effect this refers to the downside of group or team work, where members fail to adequately analyse different opinions, examine countermeasure selection and re-evaluate discarded ideas which results in poor decision making. Torma-Krajewski & Powers (2010) highlight that this phenomenon is more likely to occur in high stress environments with time constraints, where decisions are highly consequential and there is a lack of methodological procedures to develop and evaluate alternatives.

Knowledge and understanding of this phenomenon is important in the strategic stakeholder context as TRM is sometimes carried out by a team or group from different departments, including crisis management and emergency response teams. Each of which are high stress and time limited functions which can have disastrous consequences if poorly managed.

However by understanding and recognising the phenomenon, teams and senior management can implement corrective measures to prevent groupthink occurring. Torma-Krajewski & Powers (2010) suggest encouraging dissenting opinions; discussing the need to remain open to possibilities; examining patterns of decision making during previous emergencies, analysing them, and then taking corrective measures to prevent future groupthink.

Another consideration when deciding upon ownership of a TRM programme is the risky-shift phenomenon. This suggests that instead of groups or teams taking less risk by making safer or more conservative decisions, that often the opposite is the case. Mullins & Christy (2010, p. 354) highlights that, '*Studies suggest that people working*

in groups generally advocate more risky alternatives than if they were making an individual decision on the same problem.

This is not to say that there is no merit in using groups to solve problems by working together. On the contrary Shaw (cited in Mullins & Christy 2010) suggests that evidence supports the view that groups perform more and better solutions to problems than individuals. However this is an important phenomenon to consider in terms of TRM as Mullins & Christy (2010, p.354) succinctly and appropriately suggests, '*A decision which is everyone's is the responsibility of no one*'.

Risk Management

The way in which risk is managed has evolved over the last few decades and is now widely recognised as an academic discipline. The more traditional method of risk management, being departmentalised and focused mainly on hazard risks, has evolved into a more holistic and comprehensive view of a business. This wide-ranging way in which pure and business risks, are managed across a business is what is known as Enterprise Risk Management (ERM). DeLoach (2000 cited in Ward 2003, p.9) suggests ERM means that, '*a truly holistic, integrated, forward looking and process orientated approach is taken to manage all key business risks and opportunities – not just financial ones – with the intent of maximising shareholders value for the enterprise as a whole*'.

Davidson (2009, p.1) highlights that Enterprise Security Risk Management (ESRM) is a core component and subset of ERM encompassing the security related risks and concerns, and suggests that '*the goal of both ERM and ESRM is to transcend traditional management siloes to improve risk assessment and reduction*'. ESRM differs to the more generic risk management framework model such as BS 31100:2011 (Figure 1). Brooks (2011) highlights this is due to the fact that more generic risk management models focus more on probability and consequences and do not consider security concepts such as threat, vulnerability and criticality in uncertain and changing environments requiring specialist security knowledge.

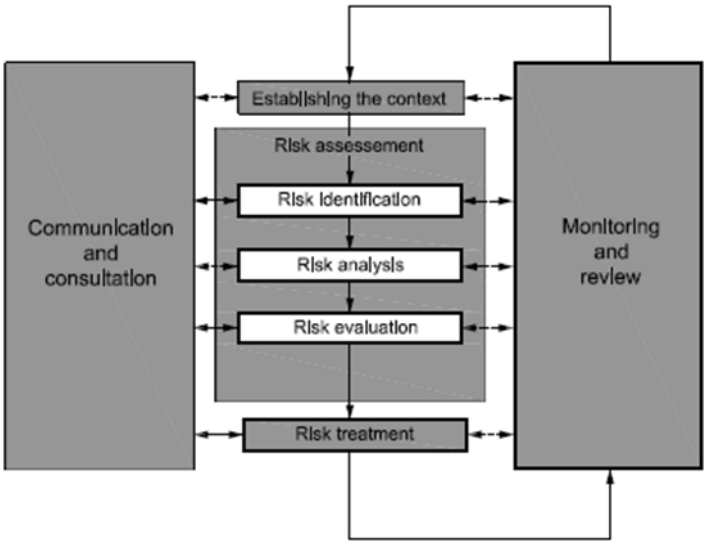

Figure 1. BS ISO 31100:2011 Risk Management Process

Source: British Standards Institution (2011, p.32)

In using an ESRM approach the operational management of risk in relation to business travel encompasses a wide range of threats, vulnerabilities and hazards. Talbot and Jakeman (2009, p.69) highlight that the '*risks to people are as varied as the countries through which people may travel'*. These include: commercial espionage; terrorism; local and transnational crime; war; health issues; weather; psychologically disturbed people.

Longmore-Etheridge (n.d) suggests that organisations also need to focus on information protection. The information and intellectual property that business travellers carry around with them in hardcopy, on laptops, tablets and smartphones is of great value and vulnerable to several forms of attack. This can take the form of technical attacks on devices such as phishing to install malware, and communications monitoring. (Dudko-Richardson 2014). It can also involve covert human intelligence gathering in airports, hotels, restaurants, vehicles and meeting locations as well as pretexting approaches and social engineering (Wilding 2009).

Another important aspect to consider is the protection of travel data from cyber-attack. Banikowski (2014) highlights that travel data contains many aspects of critical information, and that these should be protected as diligently as possible. This relates not only to an organisation, but also to their third party service providers who provide mobile device applications, and communicate/transmit sensitive information such a traveller tracking data.

The publications reviewed outline different methods of managing travel related risk. Claus (2011a, p.9) suggests an eight step plan to create an Integrated Duty of Care Risk Management Model:

1. *Plan strategically*
2. *Assess company-specific risk*
3. *Develop policies and procedures*
4. *Manage global mobility*
5. *Communicate, educate and train*
6. *Track and inform*
7. *Advise, assist and evacuate*
8. *Control and analyse*

Advito (2009, p.3) suggests a six step plan to build a Travel Risk Management Programme:

1. *Assign management responsibility*
2. *Determine risk types*
3. *Assess risk exposure*
4. *Mitigate or manage*

5. *Communicate*
6. *Audit*

Talbot and Jakeman (2009, p.69) suggest a ten step plan to ensure the safety and security of personnel travelling overseas:

1. *Define a threat-risk profile for travel destinations and monitor this regularly*
2. *Develop predefined contingency/response arrangements*
3. *Implement a compulsory notification to travel policy, which includes registering with the relevant embassy or consulate*
4. *Capture all travel details centrally*
5. *Consider intellectual property/classified material exposure*
6. *Provide overseas awareness briefings on their places of travel*
7. *Make medical check-ups, inoculations and travel/medical insurance compulsory*
8. *Implement a traveller tracking system*
9. *Provide ongoing updates throughout the person's travel period*
10. *Conduct post-travel debriefings to identify enhancements to the program*

From this it is evident that there are numerous approaches to managing business travel related risk. Borodzicz (2005) highlights that modern theorists believe that there are four key methods that can be used to deal with risks. These being the techniques of risk avoidance, risk transfer, risk reduction and risk retention. However these techniques cannot be viewed in isolation to successfully manage the risk. They need to be part of a travel security risk management programme, tailored to the specific needs of the business.

Risk Assessment

It is essential for senior management of an organisation to fully understand their risk exposure in order to identify the most effective stakeholders who will be accountable for the operational implementation of a travel risk management programme. Moreover due to the dynamic nature of the threats facing business travel it is essential that risk assessment is considered an active and continuous process. It is not a practice that can be reviewed on an annual basis. Claus (2011a, p.39) highlights that in the context of TRM a risk assessment should be conducted prior to each and every trip stating, '*Every travel approval should include an employee risk assessment component prior to departure ideally linked to the risk at the destination*'.

Contemporary organisations have two risk assessment options available to them. It can be conducted internally by 'in-house' personnel or it can be outsourced to a specialist third party provider. Claus (2011a) suggests that 'in-house' personnel will most often involve personnel from human resource, security, risk management, and/or travel departments. Ritchey (2012) also identifies the use of a threat analyst for the function. In terms of third party providers these usually take the form of a travel management company (TMC) or a specialist security/intelligence/medical service provider.

When searching through the literature for specific sources of information which could be used for travel security risk assessment purposes it became clear that academic literature on this subject is relatively sparse. Talbot and Jakeman (2009) suggest that even though many organisations have in the past relied on consular assistance or diplomatic relationships to assure the safety and security of personnel abroad, these agencies are now limited in their ability to respond due to their large workloads. Only Advito (2009) and an AIG (2011) white paper highlight that the UK Foreign and Commonwealth Office is a useful source for pre-travel risk assessment.

Advito (2009) highlights that when considering the prevalence of business travel in contemporary organisations, bearing in mind ever changing country risk profiles etc.,

there is significant expertise required and expense involved in providing continuous travel risk assessment. This may explain why the use of TMC's and transnational security consultancies in destination profiling, intelligence gathering, medical and security incident response has become much more prevalent in the last ten to fifteen years. Advito (2009, p.14) suggests it is '*almost inconceivable that a TRM program could be created and managed without outsourcing some tasks to third-party specialists*'.

Promulgation

Travel related risk can be promulgated to stakeholders by developing travel risk management policies and associated procedures, and through training. Policies provide managers and employees with a detailed guide highlighting expectations as part of overall governance and compliance. Claus (2011, p.39) also highlights the importance of an employee's '*Duty of Loyalty*' to follow policies and procedures. Traveller tracking procedures for example can infringe on a person's privacy. However their 'duty of loyalty' will ensure the business interest comes above their own.

McNulty (2013) highlights that policies are not being updated often enough and that many business travel policies address numerous issues, but not risk. A 2011 StarCite Poll (cited in Glab 2012) found 63% of companies did not have a duty of care programme in place. An AirPlus International Survey 2012 (cited in Jonas 2012) of one hundred and thirty three corporate travel buyers in North America and Europe highlights several key findings: 61% issue pre-trip advisories 16% had no safety or security component in their travel policies; 46% utilized pre-trip approval procedures; 25% conducted travel safety training; nearly 25% identified having no standard procedures for emergencies.

Another aspect to consider under the topic of travel risk promulgation is the use of pre-trip advisories or briefings. There are used for two reasons. Firstly these procedures are used to increase traveller awareness pertaining to a specific location or event. Secondly

they are used so that organisations can be seen to be pro-active in their planning against threats as travellers will normally be asked to acknowledge the receipt thereof, thus increasing compliance.

Generally pre-trip advisories will include a combination of cultural, health, safety and security related information. Advito (2009) highlights that this advisory or briefing should supply the following information: required mitigating actions; specific security tips like no-go areas; appropriate cultural behaviour; entry & exit procedures; health issues; payment methods; telecommunications specifications; internal travel by road, rail and air; emergency procedures and contacts. They also advise that a separate list should be supplied for higher-risk areas.

What is evident from examining their sample document (Appendix 1) is that it is generic in nature, whereas for a higher-risk destination much more location specific risk information would be essential. Zurich (2012) suggests that travellers should be provided with a robust set of materials which include: written notification of the risks associated with the travel; fully documented itinerary; communication plans and channels to be used; appropriate tools for communication such as roaming capability for mobile phones and mobile Wi-Fi access for laptops etc.

Whilst a pre-trip advisory is of value to the business traveller its true value can only be realised if it is combined with training. Holt (cited in Wojcik 2012) emphasises this importance stating, '*Preparing the individual is critical. If someone's experience is North America and Europe and they're going to Nigeria, you need to prepare them*'. McIndoe (2011) goes further to suggest that for an organisation this training should encompass three levels. The first being the training given to employees, secondly the training of the advisors or professionals tasked with implementing and managing the TRM programme, and finally the training of the crisis management team.

Crittenden (2012) suggests that: when unexpected security situations arise with travellers abroad, there is a marked difference in response between individuals that have

been trained and those who are untrained; when a trained traveller or expatriate faces a security or safety challenge they will respond in accordance with what they have been taught and learned, which are the protocols and pre-briefed responses, as threats present themselves; training not only teaches you how to act, but also when not to act; whilst some of the themes used in training remain constant, the training should be tailored to individual locations. However when considering the findings of Claus (2011a) in relation to the importance of business size and industry on TRM it would appear that Crittenden has not placed enough emphasis on the training being based on different job descriptions/departments and the influence of the organisations industry.

Another important aspect to consider when considering training, is information/cyber security. Only Wilding (2009) highlights specific information security risks associated with business travel and provides guidelines on how to train personnel. However none of the literature reviewed highlights the need to train business travellers how to deal with the loss or theft of a mobile device such as a tablet or smartphone, which is important as these devices, if set up and operated correctly, can be remotely located and/or wiped if necessary.

Travel security awareness training is not only being taught what the risks are and what to do if they occur, it is also about instilling a pre-emptive mind-set in the traveller in relation to their security which could reduce the likelihood of an incident occurring. Only Longmore-Etheridge (n.d) highlights specific training methods. They identify an organisation in the USA, W.W Grainger, who have established a travel security website which includes emergency contact information, nation specific travel policies and education and awareness material. They also do face-to face training with regular travellers to instil situational awareness when in a foreign country. These travellers are also supplied kidnap avoidance educational material, and for in-country employees this is escalated to kidnap avoidance and defensive driver training as part of wider risk treatment.

Risk Treatment

Organisations have four methods of risk treatment at their disposal: avoidance, transfer, reduction and retention. Not all of which can be used in every situation. Whilst risk avoidance is seemingly the most desired method of dealing with risks, it is often the most difficult to utilize as it is usually very difficult, costly, and/or limiting to implement in practice without negatively impacting on an organisation or individual. In terms of business travel security risk the only way to avoiding the risk is by terminating the practice.

In order to reduce the likelihood of an incident, or the consequences should an incident occur, an organisation will need to implement controls to ensure that the residual risk is tolerable (ALARP) and acceptable to retain. This therefore usually leaves an organisation with two options: risk reduction and risk transfer.

Pre-trip authorisation procedures are utilised as part of risk reduction. This procedure entails the use of a risk rating to grant permission, or release tickets to travellers. This may be either a manual or automated system, whereby the use of a travel risk assessment which is organisation, location and traveller specific, triggers a response. Advito (2009) suggests that a response might be as simple as a three way choice between travel being refused, approval being required or simply a briefing being required.

Advito (2009) elaborates using a case study of PricewaterhouseCoopers UK to highlight a method of pre-trip authorisation. Using this example they identify that at the point a business trip is booked, based on location, it triggers an automated series of actions. Any location with a risk level above normal will cause the tickets to be placed on hold and the organisations security department is notified to approve travel. In addition if the response is deemed to be medium level then this requires approval from a business unit leader. If it is deemed a high risk level then it will require approval from one of the heads of the three lines of the business. If it is deemed an extreme level it will require board level approval. Likewise each tier will involve different mitigating actions such

as written briefings for medium risk levels, more detailed preparation for high risk levels and intensive planning for extreme risk levels.

The use of a pre-trip authorisation system can also facilitate the restriction of the number of executives or key personnel travelling on the same flight/vessel. This is an important aspect to consider in relation to business continuity as an incident resulting in injury to, or the loss of one traveller can be severely consequential for an organisation, undoubtedly even more so if there are several personnel involved.

A global survey conducted by the Association of Corporate Travel Executives (cited in Society for Human Resource Management 2009) highlights that 84% of organisations have a policy restricting the number of executives that may travel on the same corporate or commercial aeroplane and that of these organisations 61% apply this policy only to executive level employees, 28% include all employees and 11% apply it only to corporate officers and directors. The survey also found: 40% percent of the companies limit this number to three or four; 33% allow more than ten employees to travel together; 13% limit the number to five or six; 8% limit the number to one or two. An important consideration not mentioned by the author is that for this countermeasure to be effective, it needs to be deemed, by all stakeholders, as compulsory with either its own policy or being incorporated in wider travel security policy to ensure compliance.

Another countermeasure available to organisations is the provision of an emergency contact point and associated procedures for business travellers who find themselves in trouble or in need of advice. Emergency contact procedures provide guidelines not only to the business traveller highlighting which telephone number to call, but also to emergency and crisis response teams on how to deal with a call for help in the case of an emergency.

Organisations have several options available in respect of emergency contact points. This function can be performed ‘in-house’ or it can be outsourced to an external specialist security/medical/intelligence service provider. Crittenden (2012) suggests

that the added value of using these external third party service providers to provide an emergency contact centre lies in the fact that some have intricate knowledge of a location/country after operating there for a number of years.

An organisation can also utilise an external call centre to provide a centralised contact point who then relay the information on to the relevant 'in-house' personnel. McIndoe (2011) suggests the use of a single global telephone number and/or point of contact for all emergency types is advisable in order to reduce response failures and traveller frustration. Interestingly in relation to travellers' perceived efficacy of this function, HRFocus (2008) cites results of a Control Risks Groups survey in which 36% of the business travellers identified that they had little confidence their organisations could provide reliable advice in the event of an emergency abroad.

In addition to the communication and training involved with emergency contact procedures, Advito (2009) suggests measures such as printing the emergency contact procedure and details on a credit-card sized document for the business traveller for situations where a traveller's mobile phone is damaged, out of battery life or stolen. This should also include the contact details of the relevant local Foreign and Commonwealth/Consular office. Albeit Talbot and Jakeman (2009) suggest that even though many organisations have in the past relied on consular assistance or diplomatic relationships to assure the safety and security of personnel abroad, these agencies are now limited in their ability to respond due to their large workloads.

Another risk reduction countermeasure involves the use of traveller tracking systems. These systems are of great importance as knowing the location of personnel is imperative to warn them of threats, protecting them during an incident and assisting them after an incident. McIndoe (cited in McNulty 2013) stresses their importance by suggesting that 90% of a travel risk management programme relates to traveller tracking. Zurich (2012) suggests that not only are these systems helpful in the management of travel risk, but they also demonstrate an organisation's commitment to the safety of its employees.

There are several types of traveller tracking systems in use. The first type being itinerary based systems which collate booking information relating to flights, hotels and car hire. The second being an expense related system which monitors expenditure as well as booking information. And lastly there are the technological based systems such as global positioning system (GPS) equipment or mobile technology, using real time data, to track and monitor movements. The difference between these three systems being that the first type tells you were the traveller should be, the second type tells you where the traveller has actually been, and the third type tell you where the traveller is.

Each of these traveller tracking systems has their own merit and from the review of the literature available on the subject only specialist third party service providers provide the service of utilising these systems. The use of itinerary data is useful as it helps an organisation to prevent travel to a specific location if need be. However this is dependent on the traveller booking through the prescribed channel and not making subsequent changes outside of this channel. The collation and combination of itinerary and expense related information is useful in disaster recovery situations where conventional communication methods are unavailable. However the additional use of mobile technology or GPS data is considered the most prudent in that it provides accurate location data, albeit dependent on an electronic device and power source.

Notwithstanding the fact that the technological based system is the most costly option to utilise it also introduces complications to personnel's privacy rights. Advito (2009) suggests that employers should be sensitive to privacy issues and engage in broader dialog with personnel highlighting the need and benefit of using such systems. The results of a survey undertaken by David Burnett & Associates highlight that 82% of respondents (business travellers) travelling to what they consider high-risk locations indicated that they are 'comfortable or 'very comfortable' with having their location tracked using a mobile device, and 77% indicated the same in relation to providing their location to employers using their mobile device (International SOS 2011).

Cousins (2010) highlights the development and use of specialist mobile applications to track travellers. She alludes to the various options that these applications can be tailored to suit a specific organisation. This could be by a traveller opting in to allow location data being sent automatically from the mobile device. The frequency of which can be changed dependent on the locations risk level. The location data can also be manually pushed (instigated) by the traveller. Advito (2009) elaborates to identify that these specialist applications are usually developed by travel management companies or travel security providers. Each of which are interdependent as they both need traveller booking information and destination intelligence.

Providing security updates is another risk reduction countermeasure which is dependent of technology. Just as the ability to quickly and accurately locate business travellers is important, so is the ability to quickly and reliably provide important information to the traveller. Claus (2011) suggests apart from an organisation knowing where employees are at any given time, it should have plans to communicate proactively with them if a situation changes or in the event of an emergency.

In order to provide security updates organisations have rudimentary communication methods such as phone calls, text messaging and emails as well as contemporary technological options. The first of which being that information can be pushed to travellers using the same mobile device application software which is used for traveller tracking. Secondly it can be communicated using an organisations intranet, website or social media platform. In addition Zurich (2012) identifies the use of a global distribution system. Personnel can also keep abreast of the security landscape in their location through the use of social media platforms. An example being the updates and travel advice provided by the Foreign and Commonwealth Office using the Twitter and Facebook platforms.

Risk transfer in terms of travel security risk management relates to the use of insurance. This will help to protect against the economic impact of a security incident to an organisation. This broadly falls into three types: employer's liability insurance cover to

protect the organisation in the event of a claim by an employee who is ill or involved in an accident (required by law for most employers); business insurance to provide cover for medical, security and repatriation related issues; specialist kidnap and ransom insurance for kidnap and ransom related incidents.

Employer's liability insurance cover is not only a legal requirement for most employers in the United Kingdom but also a prudent measure to protect an organisation in the event of a serious incident occurring. Winthrop (cited in HRFocus 2008) suggests that there is a real threat of legal action to corporations from travellers who feel unprotected and highlights that there have been numerous civil cases and out-of-court settlements. Claus (cited in Glab 2012) reinforces this by identifying that in her research on the topic she found that when thirty nine employees (or their survivors) sued their employer, thirty four won their case.

Business insurance products cover an organisation and business traveller. They vary significantly between insurers therefore the procurement thereof must be undertaken by key travel risk management stakeholders who take into account the traveller profile, the nature of the travel, and the length and location of the assignment in order to ensure there no exclusions or limitations to the cover. Wojcik (2012) and Zurich (2012) highlight that travel assistance programs are sometimes included in international business travel insurance products, providing security advice and support should it be required.

The provision of kidnap and ransom (K&R) insurance cover is not only a reimbursive insurance policy but can also be seen as a countermeasure. Da Silva (2012) suggests that a kidnap can have an enormous impact on an organisation as they are extremely traumatic for persons involved, can lead to significant losses from ransom payments, business interruption, litigation, adverse publicity and long-term reputational damage. Though she highlights that the real value behind a kidnap for ransom and extortion insurance is that it provides access to professional and experienced crisis response teams to assist in dealing with an event.

Procurement of K&R insurance is an important decision for an organisation as the risk of kidnap is ever-present and failure to provide this cover can result in litigation from families of victims. Crorie & Kawai (2014) highlight that even when organisations have purchased K&R insurance they are still finding themselves recipients of lawsuits. They suggest ensuring the provision of a policy with good quality response consultants to ensure situations are well managed which will reduce the risk of a liability claim.

In order to monitor and improve the effectiveness and efficiency of a travel risk management program an organisation will need to continually asses its risk landscape and evaluate the performance of risk treatment countermeasures deployed.

Evaluation

A review of the literature revealed limited information on programme evaluation specifically related to travel security. Claus (2011a) highlights that unlike other risk management activities, there are few generally accepted best practices in relation to what employers should do to assume their duty of care responsibilities. She simply highlights the need to have management controls in place to ensure employee and employer compliance, and tracking and analysing data to improve the efficiency and effectiveness of the TRM plan.

McIndoe (2011, p.3) suggests using an '*after-action review*' after any incident to determine if the issue could have been prevented or more efficiently handled. The result of which will decide if the policies, plans, procedures and mitigation strategies will need to be modified. Glab (2012) suggests an organisation calculates return on investment by carefully analysing its expatriate and business traveller population in terms of numbers travelling abroad, job function and the different risk behaviour of individuals. Barth (cited in McNulty 2013) highlights that many companies have started testing employees to ensure they have sufficient policy and safety knowledge. Advito (2009) highlights the importance of feedback from the TMC's and the individual

travellers/expatriates. They promote the use of a platform, such as a debriefing session or survey, for travellers to share experiences and tips.

Whilst these published methods of evaluation are useful they are certainly not exhaustive. Donald Kirkpatrick, Professor Emeritus at the University of Wisconsin in the USA, published in 1959 a four level training evaluation model which can be adapted to suit the function. Bates (2004, p.341) suggests that this model has been the primary organising design for training evaluations in for-profit organisations for over 30 years, stating that this model is '*By far the most popular approach to the evaluation of training in organizations today.*'

Giangreco et al (2008) highlight this hierarchical model constitutes four levels. Level one, reactions, being the emotional response to a training program not taking into account learning. Level two, learning, being the logics, methodologies and techniques acquired by trainees. Level three, behaviour, being the practical implementation of the new principles and practices learnt to modify and improve behaviour. Level four, results, being the impact of training on costs, productivity, quality or morale.

In more simple terms these levels can be described as: is the trainee happy with what they've learnt; what skills has the trainee gained; has the trainee put those skills into practice; practically what has this resulted in for the organisation. In assessing the value of this model it is evident that it can add value to the research in question by adapting it and incorporating it into the evaluation process. For example: debriefing and surveys evaluate reaction (level one); training testing evaluates learning (level two); interviews and observations evaluate behaviour (level three); analysis of key performance indicators evaluates results (level four).

Another approach to evaluation involves the use of frameworks known as capability maturity models. The Global Risk Management Committee of the United States National Business Travel Association (NBTA) in association with a specialist third part service provider, iJET Intelligence Risk Systems published a Travel Risk Maturity

Model for this purpose. This model is based on the Capability Maturity Model Integration (CMMI) developed in the United States by experts from the industry, government and Software Engineering Institute at Carnegie Mellon University.

This model provides a practical guide for organisations, and identifies five stages in the strategic evolution of a TRM strategy (Table 2). In using this model the characterisation of processes defines where an organisation is on the capability maturity continuum. Hopkin (2010) describes this type of model as a measure of the quality of risk management activities undertaken in an organisation and the extent to which they are embedded. The Advito model is valuable as it creates an evaluation benchmark with which organisations having contextual differences can be compared.

Table 2. Stages of Evolution within Travel Risk management Strategy

Maturity Level	**Characteristics**	**Consequences and barriers**
1.Reactive	Ad hoc. Few policies. Chaotic in the event of an emergency.	Organisation at substantial risk. Could incur significant liability for not fulfilling duty of care
2.Defined	Basic TRM policies defined and documented. Primary focus on incident response.	Basic elements of good strategy but not consistent. Reactive rather than proactive. Failure to reach the next level often due to reluctance to invest.
3.Proactive	Consistent execution of TRM processes.	The minimum to which organisations should aspire. Failure to reach next level is often because organisation has no enterprise-wide risk management programme.
4.Managed	Metrics collected and reviewed. Cross organisation support.	Formal program, consistently monitored with good training.
5.Optimised	Program integrated throughout organisation	Also includes process optimisation programme.

Source: adapted from Advito (2009, p.12)

In reviewing the literature associated with BTSRM it is evident that this subject is indeed as Claus (2011a, p.40) describes, '*still in its infancy*'. The aim of this research project is to bring academic credibility to the topic by examining the core components of the practice in order to determine the general level of maturity in contemporary practice.

This will involve identifying who the stakeholders are involved in current practice and how they relate to: policy creation; ownership of the practice; pre-trip authorisation procedures; incident management. Then examining: how business travel security risk is being assessed; which methods are being used to promulgate the risk to business travellers and stakeholders; how organisations are treating the risk; how organisations are evaluating their countermeasures and TRM programmes.

Chapter 3

Research Methodology

Research methodology for a research project is generally approached using deductive or inductive reasoning predicated on the philosophical viewpoint of the researcher. Broadly speaking a deductive approach involves developing theory in order to test a hypothesis. An inductive approach involves data analysis in order to develop theory. For the purpose of this project an inductive approach was used. Based on observations from the literature review and discussions with industry practitioners the research required data collection, exploration and analysis in order to reach conclusions.

The major methodological choice for a researcher relates to the use of either a quantitative or qualitative research design. Just as the philosophical assumptions of the researcher influence the research approach, the research approach influences the methodological strategy. Neill (2007) provides an accurate summary and comparison of the features of each of these research design methods (Table 3).

Table 3. Features of Qualitative & Quantitative Research

Qualitative	**Quantitative**
"All research ultimately has a qualitative grounding" – Donald Cambell	"There's no such thing as qualitative data. Everything is either 1 or 0". – Fred Kerlinger
The aim is a complete, detailed description.	The aim is to classify features, count them, and construct statistical models in an attempt to explain what is observed.
Researcher may only know roughly in advance what he/she is looking for.	Researcher knows clearly in advance what he/she is looking for.
Recommended during earlier phases of research projects.	Recommended during later phases of research projects.
The design emerges as the study unfolds.	All aspects of the study are carefully designed before data is collected.
Researcher is the data gathering instrument.	Researcher uses tools, such as questionnaires or equipment to collect numerical data.
Data is in the form of words, pictures or objects.	Data is in the form of numbers and statistics.
Subjective – individuals' interpretation of events is important, eg., uses participant observation, in-depth interviews etc.	Objective – seeks precise measurement and analysis of target concepts, eg., uses surveys, questionnaires etc.
Qualitative data is more 'rich', time consuming, and less able to be generalized.	Quantitative is more efficient, able to test hypotheses, but may miss contextual detail.
Researcher tends to become subjectively immersed in the subject matter.	Researcher tends to remain objectively separated from the subject matter.

Source: Neill (2007)

Quantitative data collection allows for large amounts of information to be summarised so that generalizations or predictions can be made. This is typically done using either surveys or experiments. Qualitative data collection provides much more detailed

information of complex situations in search of a better understanding. This is typically done using interviews, focus groups or observation. For the purpose of this project a combination of quantitative and qualitative data was required. Quantitative data allowed for generalizations regarding the problem to be made, after which qualitative data provided much more detailed data regarding the problem which then put the quantitative results into perspective.

Literature Review

Research began with an extensive literature 'trawl' covering various sociological areas on the internet using the Loughborough University Remote Working Portal to find literature relevant to the review. The searches utilized keywords and phrases in an attempt to identify all relevant literature. One of the problems encountered here was that much of the literature was related to financial and corporate social responsibility aspects, covering the research area but not the specific research problem. Another was that literature specific to the problem at hand mainly took the form of TRM as part of duty of care.

A further search for publications was conducted at the University of Westminster. Once again there were no publications aimed specifically at TRM in the context required, however numerous business management, human resources, risk and business continuity management publications provided suitable background information. In order to ensure the validity of data all online sources were checked for credibility.

Survey

Quantitative research for the project took the form of a survey. This method of collection was chosen instead of an experiment, as it allowed for information gathering from a specific sample group of practitioners with the required knowledge and

experience, in a cross-sectional manner to generalize and gain understanding of current practice and form an overview of BTSRM.

An online questionnaire (Appendix 2) was selected over a paper based system .This method was chosen as it could facilitate access to a large sample group with relative ease, it was efficient when considering the time constraints on the researcher from external influences such as work and familial commitments, and it reduced costs such as those relating to travel. Walliman (2011) also suggests that the anonymity involved in an online survey can also help to overcome bias and encourage frankness and higher response rates.

There are also potential weaknesses using this method. Walliman (2011) highlights the lack of control that the researcher has over the quality of the responses. This is due to the fact that the researcher cannot be sure that the intended recipient is actually providing the responses. There are also issues relating to sampling as random sampling methods raise concerns regarding the generalizability of results, as little is known about the population or sample reached. 'Email overload' as well as technological problems, such as 'junk' email filters may also affect response rates.

Internet based surveys also have the added complication of technical complexity. For the researcher this was not considered a problem due to proficient computing skills. Evans and Mathur (2005) identify potential weaknesses and solutions involving online surveys (Figure 2).

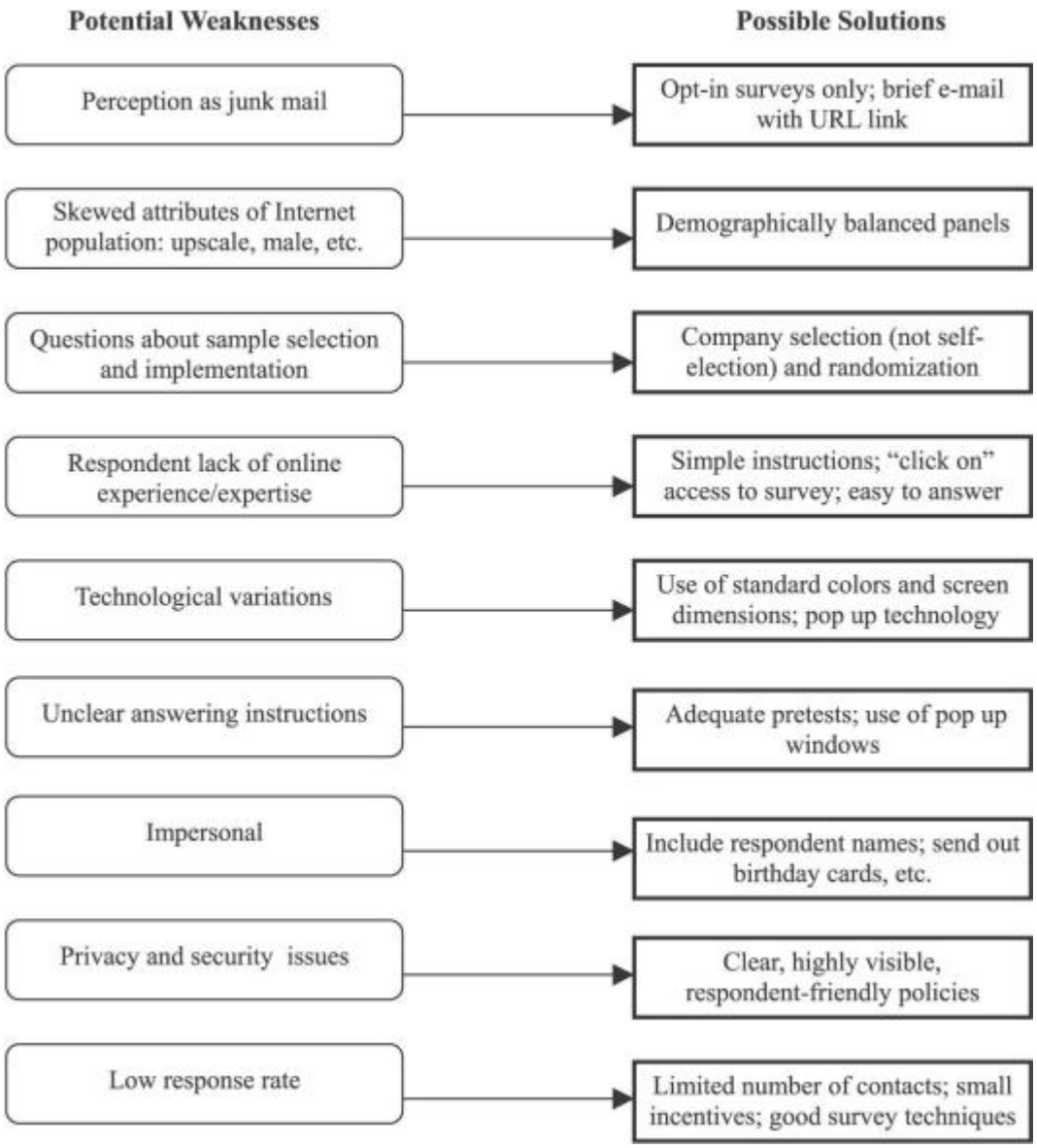

Figure 2. Addressing the Potential Weaknesses of Online Surveys

Source: Evans & Mathur (2005, p.210)

Whilst internet based surveys are preferred in order to reduce costs, there are still some costs to consider hosting the survey. This usually requires a one off payment or a monthly subscription fee. After evaluating the costs of using the SurveyMoney platform, the researcher decided that the monthly subscription cost for the hosting, which included analytical tools, outweighed the alternatives.

In order to overcome the sampling and response issues highlighted the internet based questionnaire was disseminated directly by email and social media to a target group of recognised security practitioners and business leaders, offering complete anonymity if so desired. This was carried out by the several organisations and institutions (Table 4) after making a formal request for assistance (Appendix 3).

Table 4. Online Questionnaire Distribution

Distributed By	**Institution/Organisation**	**Method of Distribution**
Security Programme Administrator	Loughborough University School of Business and Economics	Emailed directly to three hundred and sixty past and present security management master's programme students
Chapter Executive Officer	ASIS Europe UK-Chapter 208	Emailed directly to seven hundred and twenty five members
Chief Executive Officer	International Professional Security Association	Emailed directly to two hundred and eighty members
Chief Operating Officer	Association of University Chief Security Officers	Emailed directly to one hundred and forty five members
Director & Head of Commercial Directorate	The Security Institute	Publication of survey request on the closed members only LinkedIn group
The Moderator	Security Risk Management Training International (SRM-Ti)	Publication of survey request on the closed members (minimum of a masters post graduate qualification from recognised university or college) only LinkedIn group
Senior Communications Manager	Institute of Leadership and Management	Published survey request on the closed members only LinkedIn group

Source: own work, Luzzi (2014)

The survey request was also emailed directly by the researcher to eight personal contacts operating within the corporate security industry and two London based chief executive

officers of multinational corporate organisations, made possible through exposure from the researcher's current employment.

It was then decided that due to the information gleaned in the literature review, highlighting the prevalence of other key stakeholders in the management of the practice, that the sample group should be expanded to include human resource professionals to allow for more representative sampling. Obtaining access to high profile human resource institutes was particularly difficult (non-membership most frequently cited as the reason). Using a second formal survey request letter (Appendix 4) the researcher managed to obtain assistance from two personal contacts working in corporate human resource departments and the Secretary to the Council at the HR Society who emailed the survey request directly to sixty one members.

When deciding on the sample size the researcher, pre-empting a low response rate due to the sensitive and confidential nature of the topic and the researchers non-membership of the listed organisations (except for The Security Institute), decided to use the various institutes and organisations listed above in order to ensure the results gleaned sufficient data. In response to the requests made, two hundred and forty respondents undertook the questionnaire. In order to further ensure that the sample was representative, only business leaders, human resource and security professionals who operate in organisations which utilise the practice responded to the survey, the researcher included a question which would immediately exit the respondent if so indicated:

Are you, your co-workers or executives required to travel as part of your employment?

When applying this filter to the results the response level dropped to two hundred and eighteen respondents, being a total response rate as prescribed by Neumann (2005 cited in Saunders et al. 2012) of 13.96% (excluding non-targeted respondents). It was decided that should one of these respondents stop answering questions whilst completing the questionnaire that their responses would still be considered and the response rate would be automatically adjusted.

This response rate is considered by Strom et al (2010) to be low. It was also not possible to assess the efficiency of the delivery of the survey request as this was carried out by the aforementioned persons to their members. Biersdorff (2009) however states that, '*Response rate is not the best way to judge the accuracy of survey results, but representativeness is*'. In using the screening questions (1-6) in the questionnaire (appendix 2) it is evident that the respondents are widely diverse, representing organisations of different sizes and industries, functional levels and functional groups, thus ensuring representativeness.

Questionnaire planning requires several factors to be considered to ensure efficaciousness. Walliman (2011) identifies these as: establishing the exact variables upon which you wish to gather data about to ensure relevance; unmistakably clear language to prevent ambiguity; short and simple questions to reduce complexity and the effort expended by the respondent; presenting a clear and professional document encouraging response.

Evans and Mathur (2005) highlight that one of the strengths of an online questionnaire is that the researcher has control over the order in which questions are asked, with the intended progression through the questionnaire (not seeing later questions) reducing bias. Schneier (2008) goes further in studying how the psychology of decision making (heuristics and biases) affects how decisions are made. This is relevant to the planning of surveys as the order in which questions are asked and the alternatives given, can affect the responses.

The basic structure of the questionnaire is a list of questions aimed at eliciting a response which is recorded on either a checklist or rating scale. Dillman (2009 cited in Saunders et al 2012) highlight that questions will be developed based on three types of data variables: opinion; behaviour; attributes.

The research questionnaire began with an introduction (Appendix 5). Then the initial few questions related to respondent attributes such as background, business unit and

function (screening). The second phase of questions focused on behavioural attributes such as organisational structure, specific risk management practices and stakeholder involvement including opinion variables aimed at identifying perceived efficacy.

In order to ensure that the questionnaire was well structured, clearly outlined the research objectives and the importance of the project, easy to navigate and simple to answer, the researcher 'pretested' it by emailing it to two colleagues working in the security industry before attempting to distribute it. The feedback received was favourable and highlighted several questions in which improvements could be made to ensure the questions were concise and relevant. Expanding the questionnaire in length was also suggested in order to ensure it would provide sufficient data to achieve all the research objectives. These steps all being to ensure the validity of the questionnaire.

A benefit in using the SurveyMonkey hosting service is that the researcher is able at the outset of questionnaire construction to select either a compulsory or optional requirement in relation to the respondent answering a question and progressing through the questionnaire. For the survey in question respondents were forced to answer a question in order to progress through the questionnaire. This included the use of question skip logic which enabled the researcher to send a respondent to a future question based on their response to a question. For example if a respondent answered 'no' to a question they were directed to the next question, however if they responded 'yes' then they were asked further questions on the specific topic. An important benefit in using the SurveyMonkey platform is that it also includes access to analytical software to analyse results. Analysis of the data collected from the questionnaire was in the form of tables and charts. This allowed the researcher to make statistical and comparative statements.

There are several ethical issues highlighted by Saunders et al (2012) in relation to the use of an online questionnaire. These being that a researcher must: seek informed consent and agreement from participants; maintain confidentiality of data and the anonymity of participants (unless they expressly wish to be acknowledged); avoid using

the internet to share data with other participants; comply with all current data protection legal requirements. Each of these requirements having been met by the researcher

When considering a qualitative approach the researcher initially considered using a multiple case study into three or four businesses based on how Ying (2009) considers case studies the preferred strategy when 'how' or 'why' questions are being asked, when the investigator has little control over events and the focus is on a contemporary phenomenon within a real-life strategy. However his method was not selected as it would not have been generalizable, nor practicable considering the difficulty in designing a sampling framework due to varying organisational structures, industries and locations.

Interviews

The qualitative research for the project involved employing the use of semi-structured face-to-face individual interviews. Focus-group based interviews and observation were not considered practicable due to the time constraints of the project and researcher and the very large amount of data that these methods generate as highlighted by Rabiee (2004) and the University of Strathclyde (2013), as well as the sensitive nature of the topic being discussed.

For each of the semi-structured interviews a template (Appendix 6) was used to ask respondents open-ended questions. This allowed the researcher to gain further valuable insight into the topic in relation to the required research objectives. Using this method the data collection is validated due to the ability to be able to clarify questions and explore responses from different perspectives.

The advantages of using interviews are that they allow for the study of complex and sensitive areas; are useful in collecting in-depth information; non-verbal reactions can supplement a respondent's response (face-to-face interviews); reduce misinterpretation

of questions; can be used with many populations. Disadvantages include: cost implications and time consumption; data quality is dependent on the interaction between the interviewer and interviewee, which may also result in variations in response quality between interviews (Kumar 2005).

One of the major difficulties experienced by researchers in using interviews as a method of collecting qualitative or quantitative data is getting access to the desired interviewee. There may be no response to requests for interviews or access may be denied due to: confidentiality concerns; lack of interest; time constraints.

Initially the researcher aimed to approach several London based multi-national organisations who are widely known to have a large amount of personnel travelling for business purposes on a regular basis, with whom he had limited contact with through his employment. The researcher attempted to request access to the person responsible for travel risk management. However this proved to be futile as each of the organisations approached were not willing to discuss the topic due to its sensitive nature.

Therefore in order to obtain interviewees the researcher formally approached four of the questionnaire respondents, who had either actively made contact or left their particulars at the end of the questionnaire expressing interest in the topic, by email (Appendix 6). This email outlined: the scope, objectives and relevance of the study; the time required to complete the interview; the option to refuse the interview; the assurance of anonymity if requested; the availability of the study findings if so required (subject to receiving permission from the Security Management Programme Director).

In response to the requests three of the four high level respondents approached, responded positively and agreed to have face-to-face interviews on a strictly confidential and anonymous basis. Interviewee one (P1) and two (P2) both being in senior management security positions in Footsie 100 (FTSE100) organisations. The third interviewee (P3) being in a senior management risk management position in a

multi-national retailer operating in over eighty countries. The identities of the individual interviewees and their respective organisations have been provided to and verified by the researcher's supervisor, Mr Danie Adendorff. However in keeping with the agreed confidentiality and anonymity requested, their identities have not been disclosed in this dissertation.

In order for an interviewer to be effective they need to demonstrate their competence in order to be seen as credible. Saunders et al (2012) suggest that in order to achieve this, the interviewer must prepare for the interview making sure that they are knowledgeable about the research topic, that the interviewee has sufficient information to prepare for the interview and that the interview is conducted in an appropriate location. Interviews for the research were conducted at a mutually agreed time, all on the same day in London, at the relevant interviewee's offices.

Data was collected during the interviews using a tablet voice recorder application. Permission for this was requested in the researcher's preamble prior to beginning the questioning (Appendix 7). At the end of the interviews interviewees were offered a copy of the transcript to inspect. These were transcribed by the researcher (Appendix 8, Appendix 9, and Appendix 10) and edited to remove the interviewees and organisations names. This was subsequently requested by P2, provided and approved for use. A digital copy of each of the voice recordings was also provided to the researcher's supervisor, however due to the inclusion of the interviewee's names and organisations, and highly sensitive data at certain points in the interviews these were not disclosed in the dissertation.

For the data collected in the interview to be considered valid and credible Saunders et al (2012) suggest the researcher must consider several important aspects in order to avoid forms of bias: personal appearance; opening comments; questioning approach; types of questions; personal behaviour; personal attentiveness; lucidity in summarising and testing understanding; professionalism; proficiency in data collection.

When discussing the importance of survey design to data reliability Leedy and Ormrod (2010, p. 187) highlight that, "*By drawing conclusions from one transitory collection of data, we may extrapolate about the state of affairs over a longer period. At best, the extrapolation is a conjecture, and sometime a hazardous one at that, but it is our only way to generalize from what we see*". In order to ensure the internal validity of this research the researcher has utilised the triangulation strategy, whereby mixed methods are used in order to combine data to ascertain if the findings from one method mutually corroborate the finding from another method (Saunders et al 2012). In doing so 'extrapolation' has been mitigated due to the use of triangulation.

The most difficult challenge for the researcher was ensuring that the participants in the research could be considered a representative sample. In order to generate more responses the researcher considered disseminating the online questionnaire to a wide range of easily accessible business groups and forums. This approach could have generated many responses. However when taking the credibility issue previously discussed, relating to respondent identity into consideration, it was decided that the external validity of the research would be improved using a specified sample group of recognised business leaders, human resource and security professionals, contacted directly through recognised Institutes and Associations via email and social media.

The research does have its limitations in that it gives rise to concerns such as interviewee subjectivity and bias due to sample group representation size. However the researcher in consciously deciding to use triangulation to ensure the corroboration of findings from the literature review, online questionnaire and face-to-face interviews, aimed to dispel this ensuring valid and credible results.

Chapter 4

Research Findings

In this dissertation quantitative and qualitative research methods have been utilized to examine contemporary BTSRM. In order to examine and gain a representative view of current practice quantitative data collection took the form of an online questionnaire allowing a statistical analysis.

In order to assess the credibility of the questionnaire respondent data, in screening respondents were asked, '*Which of the following best describes the level at which you operate in the organisation?*' The responses highlighted a large proportion (94.04%) of the sample group being in a supervisory position or higher (Figure 3) increasing the credibility of the data received.

Q5 Which of the following best describes the level at which you operate in the organisation?

Answered: 218

Answer Choices	Responses	
Top-level (director/chairman)	**14.68%**	32
Senior-level (C-level)	**20.64%**	45
Middle-level (senior manager)	**39.45%**	86
Supervisory (manager)	**19.27%**	42
Contributor or operative	**5.96%**	13
Don't know	**0.00%**	0
Total		**218**

Figure 3. Questionnaire Response – Respondent Job Title

Source: own work, Luzzi (2014)

Semi-structured interviews with senior management representatives from three large multi-national organisations were then used to obtain qualitative data on the topic allowing the collection and examination of richer data, in order to gain a deeper understanding of the practice. In order to link the research findings to the literature review and research objectives, the results have been presented using concurring themes.

Stakeholders

When considering stakeholder involvement in BTSRM the research has highlighted that numerous functional groups are involved in the practice, not forgetting the business traveller. With this in mind it was decided that there should be two separate analyses made. The first being the stakeholder involvement when considering the organisational responsibility versus the traveller's responsibility, and the second being the variations of stakeholder involvement within organisations.

In relation to the first analysis in Figure 4 it can be seen that the respondents indicate that BTSRM should be mainly the responsibility of the organisation with input sought from the traveller, closely followed by the view that the responsibility should be equally shared by the traveller and organisation.

Q11 Who do you consider SHOULD be responsible for the management of security related risk when travelling for business?

Answered: 211

Travellers sole responsibility	Travellers responsibility with organisational support	Equal responsibility	Mainly organisations responsibility with travellers input	Organisations sole responsibility	Total
0.95% 2	**16.11%** 34	**37.44%** 79	**39.34%** 83	**6.16%** 13	211

Figure 4. Questionnaire Response – Responsibility for Management

Source: own work, Luzzi (2014)

These results are similar to the input received during the semi-structured interviews. P1 responded, '*I would say that the split is either fifty-fifty or sixty-forty, in favour of the company. The company does more but the individual should actually bring it up to fifty-fifty in reality'*. P2 highlighted equally shared responsibility but added, '*that's an interesting one. I would say it is probably not defined as much as it should be. I would say it is pretty much a fifty-fifty between the travellers themselves and the individual business unit'*. P3 also indicated that he considers it a fifty-fifty share of responsibility.

These views are similar to the findings of the Claus in relation to duty of care. '*Most respondents indicated that Duty of Care ownership is (and should be) shared between different functions in the organisation and lies (or should lie) with everyone in the company, including the employee*' Claus (2011, p.26). Claus also refers to the concept of the 'duty of loyalty' which P1 also highlighted, whereby employees must be seen to be pro-actively trying to improve their own safety and security by willingly complying with organisational guidelines, procedures and policy.

The second analysis involved examining who the key stakeholders are within an organisation in terms of functional groups. This was broken down further into

identifying who the respondents feel are, and who should be, responsible for development and implementation of a travel security policy; owning the risk; pre-trip authorisation; managing an incident.

Policy

Questionnaire respondents that indicated having a formal travel security policy were asked, '*Which department IS responsible for the development and implementation of this policy?*' (Figure 5). In order to compare results, the options provided to respondents for this question mirrored those identified by Claus (2011) and Advito (2009). The most notable result from this question being that the security department is the significantly predominant department (51.20%), rather than human resource departments (5.6%), and a significant number (13.6%) of 'other' responses highlighting departments not previously linked with BTSRM.

Q13 Which department IS responsible for the development and implementation of this policy?

Answered: 125

Answer Choices	Responses	
Human resources	**5.60%**	7
Security	**51.20%**	64
Risk management	**10.40%**	13
Legal	**0.80%**	1
Travel management	**6.40%**	8
Health, safety & environment	**5.60%**	7
Compliance & audit	**1.60%**	2
Don't know	**4.80%**	6
Other (please specify)	**13.60%**	17
Total		**125**

#	Other (please specify)	Date
1	I think it is Health and safety and HR	6/9/2014 7:51 AM
2	General	6/9/2014 7:13 AM
3	Owner	5/17/2014 5:22 AM
4	Procurement	5/15/2014 4:56 AM
5	Department of foreign affairs and international trade	5/8/2014 9:23 AM
6	All of the above	5/7/2014 11:39 AM
7	Operations	4/21/2014 1:26 AM
8	Safety and Security (One department)	4/16/2014 1:46 AM
9	more than one of the above would be responsible for developing the policy	4/15/2014 9:04 AM
10	Operations	4/15/2014 5:55 AM
11	HSES	4/15/2014 2:25 AM
12	Directors	4/15/2014 2:06 AM
13	Group Security	4/15/2014 1:50 AM
14	the departments in which staff travel as part of their main role	4/14/2014 8:14 AM
15	Insurance	4/14/2014 4:31 AM
16	Estates	4/14/2014 2:55 AM
17	Insurance	4/14/2014 1:29 AM

Figure 5. Questionnaire Response – Departmental Responsibility for Policy

Source: own work, Luzzi (2014)

When asked who ‘should be’ responsible for this function the results did vary slightly, but with the security department (49.19%) still the predominant response (Figure 6).

Q14 Which department do YOU consider most appropriate for the development and implementation of this policy?

Answered: 124

Answer Choices	Responses	
Human resources	**6.45%**	8
Security	**49.19%**	61
Risk management	**14.52%**	18
Legal	**0.00%**	0
Travel management	**8.87%**	11
Health, safety & environment	**8.87%**	11
Compliance & audit	**1.61%**	2
Don't know	**0.81%**	1
Other (please specify)	**9.68%**	12
Total		**124**

#	Other (please specify)	Date
1	Owner	5/17/2014 5:22 AM
2	All of the above	5/7/2014 11:39 AM
3	Operations	4/21/2014 1:26 AM
4	Safety and Security	4/16/2014 1:46 AM
5	Security and legal	4/15/2014 11:31 AM
6	a combination of input from more than one of the above departments	4/15/2014 9:05 AM
7	Operations	4/15/2014 5:55 AM
8	It is a collaboration between travel, security and HR	4/15/2014 3:35 AM
9	HSES	4/15/2014 2:26 AM
10	Directors	4/15/2014 2:06 AM
11	Group Security	4/15/2014 1:51 AM
12	Estates	4/14/2014 2:55 AM

Figure 6. Questionnaire Response - Preferred Departmental Responsibility for Policy

Source: own work, Luzzi (2014)

Results from these two questions vary considerably to those from the global study by Claus (2011a) where human resource departments were predominant followed by security departments. They do however concur with the results of the European study of Claus (2011b) which highlights a higher prevalence of security departments in the primary and coordination responsibility of duty of care and travel risk management in Europe.

When examining the questionnaire respondent profile it is evident that a large proportion of respondents (49.54%) are from security departments, and that the other respondents represent a diverse range of business functions (Table 5).

Table 5. Respondent Functional Group Profile

Department	**Responses**
Top-level Management	12.84%
Human resources	5.96%
Security	49.54%
Risk management	7.8%
Legal	0.92%
Health, safety & environment	2.29%
Travel management	0.46%
Operations	9.63%
Other	10.55%

Source: own work, (Luzzi 2014)

In order to estimate potential bias from respondents towards their own functional group when answering these questions a comparison of the results was conducted between two of the dominant functional groups identified (security and human resource departments). Respondents from security departments indicated their own department

being responsible 61.76% and human resource departments 28.57%. These figures drop to 56.72% and 14.29% respectively when asked who should be responsible, suggesting a low bias level.

Ownership

The next aspect of stakeholder involvement relates to the ownership of the travel security risk management function. Questionnaire respondents were asked, '*From which department IS the current risk owner (person responsible for the management of the security risks associated with business travel)?*' In response 35.78% of respondents indicate the security department currently owns the function, followed by senior management with 17.65% and then human resource and risk management departments with 6.86% (Figure 7).

Q16 From which department IS the current risk owner (person responsible for the management of the security risks associated with business travel)?

Answered: 204

Answer Choices	Responses	
Senior management	**17.65%**	36
Human resources	**6.86%**	14
Security	**35.78%**	73
Risk management	**6.86%**	14
Legal	**0.00%**	0
Travel management	**6.37%**	13
Health, safety & environment	**5.39%**	11
Operations	**3.92%**	8
Don't know	**9.80%**	20
Other (please specify)	**7.35%**	15
Total		**204**

#	Other (please specify)	Date
1	Owner	5/17/2014 5:22 AM
2	nobody as far as I know	5/14/2014 11:33 AM
3	none	5/8/2014 9:11 AM
4	Safety Management	5/7/2014 11:39 AM
5	TRAVEL IS PART OF FINANCE. NO GUIDANCE GIVEN	5/4/2014 11:58 AM
6	No responsibility assigned	4/16/2014 9:34 AM
7	there isn't one	4/16/2014 3:20 AM
8	Safety and Security	4/16/2014 1:46 AM
9	It depends. Policy, guidelines and advice pre-travel is responsibility of security dept. Once travel plans are approved, adherence to and application of security measures etc. is responsibility of the traveller and or any specialist persons required for the destination (escorts etc.)	4/15/2014 1:05 PM
10	Not addressed	4/15/2014 12:10 PM
11	Security and legal	4/15/2014 11:32 AM
12	The department that the traveller works for and the traveller	4/15/2014 3:35 AM
13	Insurance	4/14/2014 4:32 AM
14	no one	4/14/2014 3:25 AM
15	Estates	4/14/2014 2:55 AM

Figure 7. Questionnaire Response – Departmental Risk Owner

Source: own work, Luzzi (2014)

These findings again differ to Claus (2011a) and concur with Claus (2011b) in that in Europe security departments are considered to be the most appropriate risk owner followed by senior management. '*Primary and coordination responsibility in Europe lies with security followed by senior management. HR, travel and risk management are less frequently identified as owners in Europe'* (Claus 2011b, p.7).

Significantly a number of respondents identified no ownership of the function at all. A significant number of respondents (9.8%) indicated they 'don't know' who is responsible for the function. This finding correlates with the findings of Flint (2013 cited in McNulty 2013) that it is a cause for concern as people are not always sure who is in charge of risk management within corporations.

The ‘other’ responses also identified other functional groups being responsible for the function such as safety management; safety & security; insurance, finance, and estates.

This is in line with the findings of Advito (2009) who highlight that there may be various stakeholders responsible, dependent on organisational size, structure and industry.

In order to verify the prevalence of the functional groups most commonly associated with BTSRM respondents were asked to confirm the presence of specific functional groups in their organisation (Figure 8). The results of which largely concur with those highlighted by Claus (2011a) and Advito (2009). Most notably though, indicating a low level presence of travel management departments.

Q7 Does your organisation have the following dedicated departments?

Answered: 218

	Yes	No	Don't know	Total
Human resources	**87.61%** 191	**12.39%** 27	**0.00%** 0	218
Security	**80.28%** 175	**18.35%** 40	**1.38%** 3	218
Risk management	**70.18%** 153	**27.98%** 61	**1.83%** 4	218
Legal	**73.85%** 161	**26.15%** 57	**0.00%** 0	218
Health, safety & environment	**76.15%** 166	**22.94%** 50	**0.92%** 2	218
Travel management	**52.75%** 115	**45.41%** 99	**1.83%** 4	218
Operations	**84.40%** 184	**14.22%** 31	**1.38%** 3	218

Figure 8. Questionnaire Response – Departmental Availability

Source: own work, Luzzi (2014)

Interviewee's when asked the same question confirmed the presence of all the departments with the exception of P1 who identified the absence of a travel management department.

In order to determine which departments 'should be' responsible for risk ownership questionnaire respondents were then asked, '*From which department do YOU consider the most appropriate risk owner should originate?*' The results of which (Table 6) are compared to the previously identified 'current' risk owners.

Table 6. Comparison of Current and Preferred Departmental Risk Ownership

Department	**Current risk owner**	**Should be risk owner**
Senior Management	17.65%	18.32%
Human Resources	6.86%	4.95%
Security	35.78%	40.59%
Risk Management	6.86%	13.37%
Legal	0.00%	0.50%
Travel Management	6.37%	6.93%
Health, safety & environment	5.39%	5.45%
Operations	3.92%	2.48%
Don't know	9.80%	2.48%
Other	7.35%	4.95%

Source: own work, Luzzi (2014)

These results highlight notable variations in human resources, security and risk management departments. These results are inconsistent with the finding of Claus (2011a), which highlights that in relation to Duty of Care ownership few respondents pinpointed one particular function as the owner (even though HR and security were listed most often as a single owner), due to the fact that only three of the respondents

who indicated ‘other’ (of the ‘should be risk owner’), highlighted that it should be a combination of departments.

In response to the question who the current risk owner ‘is’, only P3 highlighted that they are the risk owner. P1 highlighted that the individual business unit or line manager is the risk owner, with their position being advisory:

We do not, and we stress on a number of occasions, we do not own the risk at all we are just risk advisers, and how to deal with the risk and mitigate it.

P2 highlighted that the function is ill defined as they are responsible for assessing and managing the risk, but do not consider themselves the risk owner.

When asking the interviewees who the risk owner ‘should be’ there were three different responses. P1 suggested that instead of a line manager performing the function, a new position of travel risk manager should be created and this function being part of their remit. P2 suggested that the function should be escalated to the senior manager within the individual business unit. P3 claimed to have no strong feelings on the matter as their corporate security department works closely with the human resources department, and highlighted that this would be the case even if the human resources department were to be considered the risk owner.

Pre-trip Authorisation

In order to examine pre-trip authorisation in the strategic context questionnaire respondents were asked, “*From which department is the person currently responsible for pre-trip authorisation?*” In response (Figure 9) respondents highlighted that it is mainly senior management (39.68%) and security (18.25%).

Q31 From which department IS the person currently responsible for pre-trip authorisation?

Answered: 126

Answer Choices	Responses	
Senior management	**39.68%**	50
Human resources	**4.76%**	6
Security	**18.25%**	23
Risk management	**3.97%**	5
Legal	**0.00%**	0
Travel management	**7.14%**	9
Health, safety & environment	**2.38%**	3
Operations	**6.35%**	8
Don't know	**2.38%**	3
Other (please specify)	**15.08%**	19
Total		**126**

#	Other (please specify)	Date
1	managers	6/3/2014 2:35 PM
2	Line management and possibly security	5/27/2014 10:35 AM
3	All travel is logged through the same system. Travel to high risk countries cannot be booked without prior approval. The system itself is maintained by Operations, however decision making on high risk travel is managed by the security team.	5/19/2014 9:22 AM
4	Owner	5/17/2014 5:26 AM
5	It's your own line manager	5/14/2014 11:37 AM
6	Relevant team/division director	5/14/2014 5:20 AM
7	Security & Head of Country	4/30/2014 12:35 AM
8	We call it security risk management	4/24/2014 4:06 AM
9	High and extreme risk locations must be authorised by Head of Security and line manager, all other locations by line manager only.	4/22/2014 3:06 AM
10	Travel Management and Security combined effort	4/19/2014 4:32 AM
11	High Risk - Security, Medium and below - Line Manager	4/16/2014 4:21 AM
12	two step authorisation combination of above	4/16/2014 1:04 AM
13	Mix of travel management, the traveller and security. Depending on the risk classification of the destination[s]. Low to medium risk destinations can be self-managed, high risk require corporate oversight as compulsory.	4/15/2014 1:12 PM
14	HoD in each DIRECTORATE.	4/15/2014 10:15 AM
15	program management	4/15/2014 8:35 AM

16	Low & medium risk the employees manager. High risk, the security department	4/15/2014 4:05 AM
17	Security for restricted travel countries and departmental heads for cost reasons.	4/15/2014 3:30 AM
18	Dept. / Line manager	4/15/2014 12:53 AM
19	Line Managers	4/14/2014 1:43 PM

Figure 9. Departmental Responsibility for Pre-Trip Authorisation

Source: own work, Luzzi (2014)

These results are in line with the findings of Claus (2011b) whereby in Europe security departments are more responsible for this function than other departments apart from senior management. However as also found in Claus (2011a) senior management are identified as being the most responsible for the function despite the fact that results from awareness studies indicate senior management only have a medium level of awareness in relation to duty of care and travel risk.

Questionnaire respondents were then asked, '*From which department do YOU consider the person most appropriate to manage pre-trip authorisation should originate?*' In response (Figure 10) it can be seen that there are no major fluctuations, and most notably more respondents indicated that it should be a performed by a combination of departments.

Q32 From which department do YOU consider the person most appropriate to manage pre-trip authorization should originate?

Answered: 126

Answer Choices	Responses	
Senior management	**33.33%**	42
Human resources	**4.76%**	6
Security	**20.63%**	26
Risk management	**6.35%**	8
Legal	**0.00%**	0
Travel management	**10.32%**	13
Health, safety & environment	**1.59%**	2
Operations	**7.14%**	9
Don't know	**1.59%**	2
Other (please specify)	**14.29%**	18
Total		**126**

#	Other (please specify)	Date
1	Line management and security depending on destination	5/27/2014 10:35 AM
2	Owner	5/17/2014 5:26 AM
3	Your own line manager	5/14/2014 11:37 AM
4	Relevant team/division director	5/14/2014 5:20 AM
5	Senior management and security	5/12/2014 9:11 AM
6	Security & Head of Country	4/30/2014 12:35 AM
7	Travel Management and Security combined effort	4/19/2014 4:32 AM
8	As above for Q27	4/16/2014 4:21 AM
9	Combination of responsibility. none of above adequate	4/16/2014 1:04 AM
10	As with point 30.	4/15/2014 1:12 PM
11	Fine as it is.	4/15/2014 10:15 AM
12	Senior mgmt. with input from security	4/15/2014 5:29 AM
13	As above - I set the policy!!	4/15/2014 4:05 AM
14	Combination	4/15/2014 3:46 AM
15	See 28	4/15/2014 3:30 AM
16	Combination of HSE, Security and travel	4/15/2014 1:55 AM

17	Dept. / Line manager	4/15/2014 12:53 AM
18	Line Managers	4/14/2014 1:43 PM

Figure 10. Preferred Departmental Responsibility for Pre-Trip Authorisation

Source: own work, Luzzi (2014)

All interviewees indicated that the function of pre-trip authorisation is carried out by their corporate security departments. Operationally this would however only be after their third party service provider notifies them that someone is to travel to an area, deemed by them to be medium or high risk. This however means that essentially, overall pre-trip authorisation authority has been delegated to the third party service provider.

Incident Management

The next aspect of examining stakeholder involvement involves identifying who takes ownership of a situation should a security related incident occur. Results indicate (Figure 11) that there are mainly three key functional groups involved in managing a security incident: emergency/incident response team (22%); crisis management team (21%); security department (18%).

Q27 In the event of an incident occurring who takes ownership of the situation?

Answered: 200

Answer Choices	Responses	
Emergency/incident response team	**22.00%**	44
Crisis management team	**21.00%**	42
Security department	**18.00%**	36
Human resources department	**3.50%**	7
Health, safety & environment department	**0.50%**	1
Operations	**8.50%**	17
Don't know	**10.00%**	20
Other (please specify)	**16.50%**	33
Total		**200**

#	Other (please specify)	Date
1	Me! Sole operator	6/8/2014 2:57 PM
2	SeniorManagement	6/4/2014 1:40 PM
3	Our regional company/regional structure	5/27/2014 10:34 AM
4	initial response via hotline, regional guy responds and stands up the relevant people. Usually this would be the location/country manager and his team with support from any regional teams as required. Depending on the severity of the situation, country manager may wish to delegate management to any one of the depts. listed above. But the location manager "owns" the situation.	5/19/2014 10:00 AM
5	A combination of in-house security team and outsourced providers, depending on location	5/19/2014 9:20 AM
6	Me the traveller	5/17/2014 5:25 AM
7	Line manager	5/14/2014 11:40 AM
8	depends on incident type	5/14/2014 11:36 AM
9	Government department DFAIT	5/8/2014 9:25 AM
10	whichever senior management person is available	5/8/2014 8:23 AM
11	We are a small company so it'd be the directors	5/8/2014 2:31 AM
12	Probably Manager in UK. Senior manager and myself travel	5/7/2014 7:25 AM
13	Regional SVP	5/6/2014 5:45 AM
14	Senior Mgmt.	5/6/2014 12:50 AM
15	it can escalate from security dept. to Crisis Team + Security Dept.	4/24/2014 3:06 PM
16	Myself and colleagues coordinate a suitable response	4/24/2014 2:29 PM
17	it is joint Security Risk Management	4/24/2014 4:05 AM

18	Security team, plus the crisis mgmt. team if required.	4/21/2014 10:51 AM
19	Security initially, then the BU crisis team at the asset/country	4/19/2014 4:31 AM
20	SeniorManagement	4/18/2014 8:54 AM
21	Varies according to the hours in which the emergency may arise.	4/17/2014 1:57 AM
22	Probably no-one	4/16/2014 9:35 AM
23	As yet no incidents have occurred involving overseas travel although I believe HR would take the lead	4/16/2014 2:21 AM
24	Safety and Security	4/16/2014 1:48 AM
25	Command and Coordination Center	4/16/2014 1:03 AM
26	Security or Crisis Management Team dependent on the scale of the incident	4/16/2014 12:03 AM
27	No one would know. It would be chaos.	4/15/2014 11:21 AM
28	a combination of the above departments - dependent on nature of incident	4/15/2014 9:09 AM
29	Varies client by client	4/15/2014 9:01 AM
30	Insurance Company	4/15/2014 4:59 AM
31	We have a Tier system incident-crisis	4/15/2014 2:29 AM
32	Directors	4/15/2014 2:08 AM
33	depends on the nature of the incident. Can be Crisis management, the fire alarm team, the Health, safety & Environment department or external first responders such as the police or the fire brigade	4/14/2014 6:38 AM

Figure 11. Incident Management

Source: own work, Luzzi (2014)

In response to this question P1 highlighted that their human resources department would '*take the lead*' unless it is a serious security incident, then the security department would be called in to assist in the response, as part of a crisis management team.

P2 highlighted that the global business continuity department would manage and share responsibility for an incident with the global security department, seeking input from other functional groups as a team, when required and based on the type of security incident.

P3 explained that his organisation has a specific system used for business continuity management which involves key leaders within the organisation, including corporate

security and risk management departments, and that this system managed by senior management is also used for crisis management.

These findings once again concur with Claus (2011b) in that coordination responsibility in Europe lies with security departments, and less with human resource departments as found in Claus (2011a). Interestingly 10% of questionnaire respondents indicated they 'don't know' who will take ownership of a situation. This result is significant when considering the selected sample group. These results once again echoing the concerns of the earlier cited Flint (2013).

Advito (2009) suggests that organisational size and structure is an important influence on travel risk management. In order to examine the influence of the business size on who coordinates a response to a security incident, a comparison was conducted by filtering results by organisational size. The results confirming that the majority (85.88%) of respondents who indicate having an emergency/incident or crisis management team being from large organisations.

Risk Assessment

In order to examine the ways in which organisations assess the risk facing their business travellers the questionnaire focused on several aspects. Is risk assessment done internally or outsourced, how are the risks identified and what criteria are used for risk evaluation?

Questionnaire respondents were first asked, '*In your organisation how is the travel security risk assessed?*' Respondents indicated (Figure 12) that 65.84% conduct risk assessment internally and 20.30% outsource this to a third party service provider. A significant result from this question is that 13.86% of respondents indicate they 'don't know' how the risk is assessed in their organisation. This is once again significant when considering the profile of the sample group.

Q18 In your organisation how is the travel security risk assessed?

Answered: 202

Answer Choices	Responses	
In-house	**65.84%**	133
Outsourced	**20.30%**	41
Don't know	**13.86%**	28
Total		**202**

Figure 12. Risk Assessment

Source: own work, Luzzi (2014)

In order to examine if the use of outsourcing may be dependent on the size of the organisation a filter was place on the results of those respondents indicating outsourcing. This result highlights that 80.49% of those outsourcing the function are from large organisations. This was also the case with all three interviewees who confirmed utilising the services of a third party service provider.

For the purposes of travel security risk assessment many organisations and third party service providers categorise and rank the level of risk traveller's face. The result of this evaluation may for example take the form of a rating in order of risk level, one through to five or a high, medium or low rating.

In order to test the familiarity of these ratings questionnaire respondents were asked, '*Does travel for your organisation involve any medium or high risk locations?*' In response (Figure 13) to this 73.76% indicated 'yes', 22.28% indicated 'no' and 3.96% indicated they 'don't know' indicating a significant understanding of the terminology in use, as well the prevalence amongst respondents of travel to medium and high risk locations.

Q20 Does travel for your organisation involve any medium or high risk locations?

Answered: 202

Answer Choices	Responses	
Yes	**73.76%**	149
No	**22.28%**	45
Don't know	**3.96%**	8
Total		**202**

Figure 13. Risk Levels

Source: own work, Luzzi (2014)

Interviewees expanded on the use of these ratings and risk assessment. P1 explained that when using a third party service provider, countries are rated on a sliding scale from one to five, where five is the most high risk country. They are then informed by the service provider of any travellers intending to travel to countries rated four or five, to assess if mitigation measures are necessary or to avoid the risk completely by banning travel. The problem however highlighted by the interviewee in using external companies for risk assessment, is that if a comprehensive travel security program is not in place, which has a compulsory notification to travel policy, travellers may be making bookings outside of the third party service provider and the risk associated with their intended travel is unassessed.

P2 initially indicated the use of multiple sources for risk assessment. However it became apparent during the course of answering the question that the overarching assessment was provided by their third party service provider:

We obviously use our own data that we have got globally, we have offices based in forty six countries, so we can get that in country information as well. Most of it comes in from a security perspective from external stakeholders, Ijet we would use, as I say

Government foreign offices, media, social media, all those. It's one big pool of data and see what comes out of the middle of them then really. So I think Ijet is our main tool in how we factor whether we travel to a region or not so they score from one to five, one's lowest, five's highest. So if it's a five we are talking places like Iran, Afghanistan which we haven't got business in, but they are no goes for us. Four is a high risk so something like Bangkok or Thailand who recently went up to a 4 because of all the civil unrest or Ukraine or something like that. So that's what we gauge our travel on because it's consistent globally and it delivers the same message, it's based on the same criteria. We can override it, we can upgrade it or downgrade it if we think there is less risk or more risk but that's pretty much what we use as a business.

P3 highlighted the high level of dependency on a third party service provider for risk assessment. If the service provider increased the risk level of a particular country, then this would in turn result in further examination, in conjunction with the service provider, on the impact on travellers and future travel to the location:

It's majority out sourced basically. We use that to a large degree to assess the risks, then if particular countries or areas become more high risk then we would have a more in depth conversation, probably with the third party provider.

In order to identify which sources of information are used for risk assessment, respondents who conduct travel security risk assessment internally were asked, '*What sources of information are used for this assessment?*' Respondents indicated (Figure 14) the use of the Foreign and Commonwealth Office (68.42%), the media (52.63%), free online resources (47.37%) and industry networks (57.14%). Significantly once again 15.04% indicated they 'don't know'. As this question allowed respondents to select a number of options a considerable number (36.84%) of respondents indicated 'other' sources.

Q19 What sources of information are used for this assessment?

Answered: 133

Answer Choices	Responses	
Foreign & Commonwealth Office (including the Overseas Business Risk service)	**68.42%**	91
Media (including social media)	**52.63%**	70
Free online resources	**47.37%**	63
Industry networks	**57.14%**	76
Don't know	**15.04%**	20
Other (please specify)	**36.84%**	49

#	Other (please specify)	Date
1	Internal analysis teams	6/14/2014 10:40 AM
2	Australian equivalent of FCO, defence advisories	6/12/2014 12:47 AM
3	Contracted external providers	6/9/2014 11:27 PM
4	United Nations, US State Dept. Travel Advisories	5/26/2014 4:56 AM
5	also subscribe to iJET, Control Risks and other sources as well as liaison with embedded peers.	5/19/2014 9:57 AM
6	Anvil and International SOS	5/19/2014 9:19 AM
7	Personal recommendations	5/19/2014 3:52 AM
8	Intelligence analysis and risk assessments	5/15/2014 4:15 AM
9	Control Risks Group	5/15/2014 2:03 AM
10	Department of Foreign Affairs	5/14/2014 9:55 AM
11	Intelligence Sources - Armed Forces	5/14/2014 9:13 AM
12	travel security risk providers	5/12/2014 9:06 AM
13	Nothing really	5/8/2014 2:30 AM
14	CAA & EASA	5/7/2014 11:40 AM
15	In-country sources	5/7/2014 3:32 AM
16	Contextual contacts (e.g. people in-country)	5/6/2014 12:50 AM
17	Other government departments	5/4/2014 7:46 AM
18	ijet, CRF, OSAC, ASIO, Stratfor, think tanks, staff	4/24/2014 3:04 PM
19	trusted local assets	4/24/2014 2:27 PM
20	Risk advisory service	4/22/2014 10:34 AM
21	Travel risk software platform	4/21/2014 10:49 AM
22	paid for consultative resources	4/19/2014 4:29 AM

23	contracted information service providers	4/16/2014 4:35 AM
24	Security intelligence provider	4/16/2014 2:22 AM
25	Personal networking channels	4/16/2014 1:47 AM
26	Police and intelligence	4/16/2014 1:02 AM
27	Specialist foreign intelligence providers, US govt. resources	4/16/2014 12:02 AM
28	Own intel and analysis dept.	4/15/2014 10:39 PM
29	iJET, Red 24, OSAC, CRG, Our own people deployed globally, security representatives of our customers	4/15/2014 1:07 PM
30	Stratfor, OSAC	4/15/2014 12:44 PM
31	Partners	4/15/2014 12:10 PM
32	Intelligence suppliers	4/15/2014 11:21 AM
33	CIA website, Control Risks	4/15/2014 9:00 AM
34	Multi-agency approach	4/15/2014 8:07 AM
35	External Agents	4/15/2014 5:48 AM
36	other government sites, external travel security provider	4/15/2014 4:42 AM
37	CR & ISOS travel advisories	4/15/2014 4:03 AM
38	Professional travel and medical support services	4/15/2014 3:43 AM
39	Outsourced intel and alert data services	4/15/2014 3:29 AM
40	Group Situation Centre in HQ with Localized Situation Centre's across the globe	4/15/2014 3:10 AM
41	Government Agencies	4/15/2014 2:40 AM
42	Local source information	4/15/2014 2:39 AM
43	Outsourced service as well question 17 should have had this	4/15/2014 2:28 AM
44	Service Providers such as ISOS and Anvil plus Internal Intelligence Group	4/15/2014 2:25 AM
45	UN security briefings	4/15/2014 2:07 AM
46	In-house analysts	4/15/2014 2:05 AM
47	External specialist advisors	4/15/2014 2:01 AM
48	Insurance company support and Red 24	4/14/2014 8:16 AM
49	Professional sites provided by our insurers	4/14/2014 2:56 AM

Figure 14. Risk Assessment Information Sources

Source: own work, Luzzi (2014)

Several of the 'other' responses indicate the use of third party service providers to some extent which indicates that the results of the previous question indicating the rather low use of third party service providers could possibly be underestimated.

In analysing the data it is evident that there are numerous channels and options available to organisations to assess the risk they face in relation to travel. An important point that needs to be considered however is bias. This may be found in the way in which a third party service provider assesses the risk of a particular location, as the provider being utilised may also be assisting with risk mitigation measures and therefore it would be in their best interests to over-estimate potential risk. Likewise Wirz (2012) highlights there may be bias in travel advisories issued by governments for political and/or economic reasons.

Promulgation

In order to analyse how organisations promulgate the security risks associated with business travel prior to travel, several aspects were analysed. These being policy, pre-trip advisories/briefings and training.

Policy

In order to examine current practice in relation to policy, questionnaire respondents were asked, '*Do you have a formal travel security (or similarly entitled) policy and associated procedures?*'

The results (Figure 15) highlight 60.48% indicated 'yes', 34.29% indicated 'no' and 5.24% indicated they 'don't know'.

Q12 Do you have a formal travel security (or similarly entitled) policy and associated procedures?

Answered: 210

Answer Choices	Responses	
Yes	**60.48%**	127
No	**34.29%**	72
Don't know	**5.24%**	11
Total		**210**

Figure 15. Questionnaire Response – Formal Travel Security Policy

Source: own work, Luzzi (2014)

In the absence of having directly comparable figures these results are seen to be considerably poor and very much in keeping with McNulty (2013) who suggests that many business travel policies do not address risk. HRFocus (2008) indicates that forty-six percent of travellers in a United States business study highlighted they have no clear travel security policy.

The questionnaire respondents who responded with 'no' or 'don't know' to having a dedicated travel security policy and procedures were then directed to another question. '*Are business travel security risks a sub-component of any other policy which you have in place?*'

Responses to this follow on question (Figure 16) indicated the following policies: risk management (19.28%); travel (18.07%); security (14.46%); other (21.69%). Once again a significant number of respondents (33.73%) indicated they don't know and the majority of the respondents who indicated 'other' stated 'no'.

Q15 Are business travel security risks a sub-component of any other policy which you have in place?

Answered: 83

Answer Choices	Responses	
Risk management policy	**19.28%**	16
Travel policy	**18.07%**	15
Security policy	**14.46%**	12
Don't know	**33.73%**	28
Other (please specify)	**21.69%**	18

#	Other (please specify)	Date
1	Travel Guidelines	6/1/2014 4:26 AM
2	Insurance stipulations	5/19/2014 3:51 AM
3	No	5/14/2014 12:31 PM
4	no	5/8/2014 9:11 AM
5	The question is a yes/no answer but the options are multiple choice. The answer is 'No'.	5/6/2014 12:48 AM
6	NO BUSINESS TRAVEL SECURITY POLICIES	5/4/2014 11:58 AM
7	No	4/18/2014 9:58 PM
8	No	4/16/2014 9:33 AM
9	no	4/16/2014 3:19 AM
10	HR	4/16/2014 2:18 AM
11	No	4/15/2014 1:28 PM
12	No	4/15/2014 12:10 PM
13	Not much elaborated at all.	4/15/2014 10:12 AM
14	No	4/15/2014 10:12 AM
15	My Clients are generally poorly equipped and educated in this matter	4/15/2014 8:58 AM
16	Health and safety policy	4/15/2014 6:00 AM
17	no	4/14/2014 3:25 AM
18	None	4/14/2014 1:20 AM

Figure 16. Questionnaire Response – Inclusion in Associated Policies

Source: own work, Luzzi (2014)

These two sets of results are put into perspective by the responses from the interviewees. P1 provided interesting insight when asked if they had a dedicated travel security policy:

I can tell you in one word what our policy is, fragmented. We have a very high level policy of, as I mentioned, you are encouraged to use Ijet. If you don't use one of the main travel agents, the MTA's, that are linked into Ijet then we encourage you to put the data on, or you should put the data on manually onto Ijet. It doesn't happen, a lot of the time it just doesn't happen on the manual entries. Automatic entries no problem, and the people know which ones those are, so that at the top level is very cuddly, it is very friendly approach, we are not a big ogre that puts out black and white which is in some cases unfortunate. So we have a top level strategy of advising people what our policy is per say. It is what to do in the event of an emergency, where to go, how to do that, and behind the scenes the policy for me is that I have protocols with both Ijet and any of my security command centres 24/7 that Ijet will phone into. So we do that, but as far as the user is concerned it is fairly transparent and it is fairly hands offish by the big bad ogre of corporate. So there is no definitive travel policy, if you said to me what is our travel policy in the book? There isn't one, and if there is it will be in a division only, it won't be across all the businesses. So unfortunately, fragmented.

P2 highlighted having no dedicated travel security policy however that travel security risks were included in other policies:

So in part it comes under the global security policy, in part it comes under the global travel policy but we don't have that policy in the middle which is a dedicated travel security policy. It is currently being written at the moment. It is something that we are working through at the moment, writing a dedicated policy just for travel security. But one of the issues goes back to your previous question around who owns that policy, so that is an interesting one.

P3 also highlighted that they had no dedicated travel security policy, but more travel advice:

I think there is kind of advice, whether or not you would call it an actual policy, I don't think so. It's documented as a policy I think for certain criteria and briefings etc., which you could technically argue is policy, but it's not actually called that, it's called travel advice.

Pre-trip Advisories

Questionnaire respondents were asked, "*Does your business provide business travellers with a pre-trip advisory or briefing*". The responses (Figure 17) highlight 67.82% indicating 'yes' and 32.18% indicating 'no'. This result is very similar to that of the AirPlus International Survey 2012 (cited in Jonas 2012) in which 61% of respondents highlighted they issued pre-trip advisories.

Q21 Does your business provide business travellers with a pre-trip advisory or briefing?

Answered: 202

Answer Choices	Responses	
Yes	**67.82%**	137
No	**32.18%**	65
Total		**202**

Figure 17. Questionnaire Response – Pre-Trip Advisory/Briefing

Source: own work, Luzzi (2014)

P1 when discussing pre-trip briefings highlighted limited advice being given to travellers:

O*ne small business does pre-travel advice, in-effect goes through a questionnaire, none*

of the other businesses do. So the vast majority of people will get no other pre-travel advice apart from that which is pushed by Ijet itself which is a failing on our part.

P1 also identified a significant problem which relates to the automated process of pre-trip advisories being issued by the third party service provider. The interviewee highlighted that if the traveller does not make the travel booking using the prescribed channels the third party service provider is unaware of the intended travel plans and no pre-trip advisory is dispatched:

The problem that I have with Ijet is that the travel data collection through Ijet is not compulsory in our company, it is not mandatory. So if you happen to use a travel agent that is linked into Ijet all well and good, if you don't or if for example you go on the web and book a low cost airline it is down to the individual who is encouraged to manually enter that data. Now if you are looking at a travel planner or PA, most of the PA's around the bazaars are ok, they try and do it, but if you are looking at individuals, middle managers who don't have that admin support they won't do it.

P2 identified a third party service provider as being responsible for issuing the pre-trip advisory. The interviewee highlighted similar problems to those identified by P1:

So we book all travel through Amex. That feeds into Ijet and that's where it will get captured. There are countries in the world who can't use Amex for whatever reason and they would book direct, and that's where some of these things fall down, where people can book a flight direct with an airline or through Expedia or something like that because it's cheaper. There is an option to allow us to manually input a trip so if I booked a flight direct then I can manually put my trip into Ijet, but it is not compulsory.

P3 highlighted the fact that in their organisation the travellers are responsible for the retrieval of the pre-trip advisory. It is not a fully automated process. The traveller is

merely sent an automated reminder to access and retrieve the relevant location and or security information:

Everybody who travels has access to it and every time they book they get a reminder of what website to look onto and a reminder about the app.

P3 did highlight a slight difference to the other two interviewee's in that in their organisation it is policy and compulsory, to book all travel through a specific travel company.

Training

Training in context refers to awareness, emergency and compliance training. Questionnaire respondents were asked "*Does your business provide security specific training for its business travellers?"*

The results (Figure 18) highlight 42% indicating 'yes' and 58% indicating 'no'. These poor figures correlate with the suggestion of McIndoe (cited in McNulty 2013) that despite the high return on investment of training initiatives, training is the risk management component which has the least spent on by companies.

Q23 Does your business provide security specific training for its business travellers?

Answered: 200

Answer Choices	Responses	
Yes	**42.00%**	84
No	**58.00%**	116
Total		**200**

Figure 18. Specialised Security Training

Source: own work, Luzzi (2014)

In comparison, in the Inform Logistics survey (cited in McNulty 2013) 17% of respondents highlighted that their firms provided pre-travel risk training and 23% provided crisis and emergency management training.

In order to improve this Pocus (cited in McNulty 2013) highlights the importance of adopting comprehensive training initiatives for all new hires and that getting them in really early on in the process is extremely important.

Questionnaire respondents who indicated their organisation did security specific training were then asked, "*Is this provided for in-house or outsourced?*"

The results (Figure 19) highlight 76.19% indicating this being conducted 'in-house', 22.62% indicating it being 'outsourced' and 1.19% indicating they 'don't know'.

Q24 Is this provided for in-house or outsourced?

Answered: 84

Answer Choices	Responses	
In-house	**76.19%**	64
Outsourced	**22.62%**	19
Don't know	**1.19%**	1
Total		**84**

Figure 19. Responsibility for Training

Source: own work, Luzzi (2014)

P1 identified having a formal training programme using a third party company. However this currently does not focus on travel or any of the associated risk. The interviewee did highlight that there are plans for it to do so, which will include educational videos and a website. The interviewee highlighted that no specialist training such as hostile environment awareness training (HEAT) or contractors on deployed operations training (CONDO) is given either.

P2 highlighted that they only conduct security specific training when specifically requested to do so, and this usually relates to expatriates going on a long term assignment. The interviewee alluded to the fact that a computer based training programme, highlighting basic security advice is currently under consideration. The interviewee also identified not currently using any HEAT or CONDO training, however that could soon be reviewed:

No, we don't go to that many locations which require it but saying that all the emerging markets are in the high risk countries at the moment and we are starting to branch more into mid-Africa and places like that which potentially could change things a little bit I think.

P3 highlighted providing in-house general security awareness training for all business travellers. These sessions are also used to promote the risk reduction tool (mobile application) on offer and to remind them of their obligations. The interviewee also highlighted that no HEAT or CONDO training is conducted due to their low risk appetite in relation to travel security risk and the nature of their operations.

Risk Treatment

There are several risk reduction options available to modern day organisations to reduce the likelihood of a travel security incident occurring and or to reduce the impact of an incident should an incident occur. This can include the use of 'in-house' security personnel or third party security companies to supply close protection or executive protection services. However due to the limited scope of this research an examination of this method of risk reduction has not been included. The risk reduction methods focussed on in this research are compulsory pre-trip authorisation procedures, emergency contact procedures, traveller tracking techniques and traveller security updates.

Compulsory Pre-trip Authorisation

Questionnaire respondents were asked, '*Does your organisation have a compulsory pre-trip authorisation procedure?*'

In response 63.82% of respondents indicated yes, 29.15% indicated no and 1.88% indicated they don't know (Figure 20).

Q30 Does your organisation have a compulsory pre-trip authorisation procedure?

Answered: 199

Answer Choices	Responses	
Yes	**63.82%**	127
No	**29.15%**	58
Don't know	**7.04%**	14
Total		**199**

Figure 20. Compulsory Pre-Trip Authorisation Procedure

Source: own work, Luzzi (2014)

In comparison the AirPlus International Survey (cited in Jonas 2012) highlighted the confirmation of pre-trip approval procedures at 46%, and Claus (2011a) at 66%. The questionnaire results are somewhat higher than the 46% identified in the AirPlus International Survey 2012 (cited in Jonas 2012). However in their survey respondents were only asked who utilised pre-trip approval procedures, and not specifically if there was a compulsory pre-trip authorisation procedure.

P1 confirmed having a compulsory pre-trip authorisation procedure. This procedure is initiated for travellers who are travelling to locations deemed high or extremely high risk by their third party service provider. The interviewee however highlighted the limited effectiveness of this procedure as it is not compulsory for travellers to use travel agents who are linked to the third party service provider:

The problem that I have is that the travel data collection through Ijet is not compulsory in our company, it is not mandatory.

P2 highlighted only having a compulsory pre-trip authorisation procedure for certain countries therefore having a limited effect as it is not compulsory to use the prescribed travel agent:

Only on certain criteria. So if it is a high risk country or if it is a country where we blocked travel.

P3 highlighted having a compulsory pre-trip authorisation procedure for high risk locations only, and it being compulsory under the general travel policy to book all travel through the approved travel booking company. However when elaborating on the topic the interviewee identified a lack of confidence in their programme:

Actually they could just go outside the travel company and make travel arrangements and if they chose not to tell anyone within the company then we wouldn't know, but we certainly make this strong advice or policy that they must book all travel through the company.

Another aspect of pre-trip authorisation is limiting of numbers of key personnel or executives on an aircraft/vessel. This aspect was purposely not included in the questionnaire due to its highly confidential and close relationship with kidnap and ransom insurance, however interviewees elaborated on the complexity of the practice.

P1 highlighted that they do try and limit the numbers of key personnel travelling together but it is not enforced:

It is hugely difficult, because a) you don't know if some of them are flying or not, b) you have this siloed division so a divisional director may say I only want four of my guys in the whole division to travel on the same plane. But another division has another four guys so we at corporate level, at the high level go hey guys, hold on you can't do this

and they come back and say, well actually we can afford to lose four guys and the other division can afford to lose four guys, and this is how they think, but so in theory actually thank you very much but we're ok. So that is their risk assessment and I have that almost on a daily basis I have that argument, and I get my Ijet notifications I look at anything rated over four, I don't actually do anything with fours but I do with five and definitely six, seven, eight, nine and tens. We had our company conference recently and I had exactly that argument people saying and this is the top one hundred people in the company all flying to Singapore. Usually Singapore is fairly restrictive airspace so you have these optimum BA flights that they were travelling on and I had that that answer back, that we had maybe ten people on the flight but only three of them were specialist in this area three of them are specialist in that area. Devastation to the company, as I believe it was with MH370 and I can't remember I might be misquoting but I thought it was IBM, one of the big companies had a number of people on there and it doesn't matter whether they are good at a particular role, the devastation across the company is huge. Yes we do, is it well enforced, no it is not.

P2 highlighted problems with enforcing a limit and that this does not fall under any policy:

We try to but financially the more people you put on a specific aeroplane the cheaper the seats become unfortunately. We have an unwritten rule of twenty five or over is too many, to keep it below that, we also try to restrict the exec's travelling all on the same plane or whatever, just in case something happens but it is not enforced as well as it probably could be.

P3 did not allude to any complexity, identifying that this practice is covered by the organisation's travel policy which restricts the total number of personnel travelling based on the total number of passengers, their job function and level within the organisation.

Emergency Contact Point

Questionnaire respondents were asked, '*Does your organisation have a dedicated 24/7/365 contact point in the event of an emergency or crisis situation*?

In response 80% of respondents indicated 'yes', 17% indicated 'no' and 3% that they 'don't know' (Figure 21). Once again the 3% indicating they don't know is a concern when considering the profile of the sample group and the fundamental importance of the question.

Q25 Does your organisation have a dedicated 24/7/365 contact point in the event of an emergency or crisis situation?

Answered: 200

Answer Choices	Responses	
Yes	**80.00%**	160
No	**17.00%**	34
Don't know	**3.00%**	6
Total	**200**	

Figure 21. Dedicated Emergency Contact Point

Source: own work, Luzzi (2014)

These figures indicating the use of contact points are significantly better than the 30% figure highlighted in Jonas (2012) from the AirPlus International Survey. Respondents who responded 'yes' to having an emergency contact point were then asked, '*Is this provided for in-house or outsourced*?' In response 68.5% indicated it being provided 'in-house', 29.38% indicating it being 'outsourced' and 1.88% indicating they 'don't know' (Figure 22).

Q26 Is this provided for in-house or outsourced?

Answered: 160

Answer Choices	Responses	
In-house	**68.75%**	110
Outsourced	**29.38%**	47
Don't know	**1.88%**	3
Total		**160**

Figure 22. Responsibility for Emergency Contact Point

Source: own work, Luzzi (2014)

P1 highlighted that their organisation has a full time company branded emergency contact point with a dedicated system of protocols in place to deal with situations. The contact details of which are provided to the traveller upon registration of a proposed trip with the third party service provider, with severe incidents relayed to the United Kingdom or Canada Offices. The interviewee highlighted that their aim is to quickly have the traveller relayed to a person responsible, who in their organisation is part of the human resources management:

So within ten minutes there should be somebody saying I know who you are, I know where you work, I am prepared to help.

Importantly this method of managing emergency situations is dependent on the organisation and third party service provider being aware of the travel, in order to provide the traveller with the relevant contact details. P2 and P3 both confirmed that they have an emergency contact point and that these are fully managed through their third party service providers. McIndoe (2011) highlights the importance of having a round the clock contact point for emergencies, and the need for a response plan with protocols in order to deal with the situation.

Traveller tracking

In order to identify the extent of the use of traveller tracking and gain insight into the methods organisations use, questionnaire respondents were asked three questions. The first of which being, '*Are business travellers actively tracked during travel?*'

In response 37.88% indicated 'yes', 55.05% indicated 'no' and 7.07% indicated they 'don't know' (Figure 23).

Q33 Are business travellers actively tracked during travel?

Answered: 198

Answer Choices	Responses	
Yes	**37.88%**	75
No	**55.05%**	109
Don't know	**7.07%**	14
Total		**198**

Figure 23. Active Traveller Tracking

Source: own work, Luzzi (2014)

These poor results are similar to that found in Claus (2011) where 36% of respondents highlighted that they know where employees are at all times and can locate them immediately if requested, and that 46% of respondents indicated tracking employees through a travel tracking system. Once again the percentage indicating they 'don't know' is concerning when considering the profile of the sample group.

McIndoe (cited in McNulty 2013) suggests that the result of the Inform Logistics survey, which highlights that 52% of respondents described their company's response

to major disasters as reactive, compared to the 34% describing it as proactive, being due to respondents relating the importance of traveller tracking to the perceived efficacy of the risk management.

Questionnaire respondents who indicated actively tracking travellers where then asked, '*Is this provided for in-house or outsourced?*' In response 53.33% indicated 'in-house' and 46.67% indicated 'outsourced' (Figure 24).

Q34 Is this provided for in-house or outsourced?

Answered: 75

Answer Choices	Responses	
In-house	**53.33%**	40
Outsourced	**46.67%**	35
Don't know	**0.00%**	0
Total		**75**

Figure 24. Responsibility for Traveller Tracking

Source: own work, Luzzi (2014)

Glab (2012) highlights that when outsourcing traveller tracking, the larger the organisation the cheaper it becomes. In order to examine the influence of organisational size on uptake, a comparative filter was applied to the results. The results of which (Figure 25) indicating that there is indeed significantly higher use of outsourcing amongst large organisations, than in medium and small organisations.

Q34 Is this provided for in-house or outsourced?

Answered: 75

	In-house	Outsourced	Don't know	Total
Q1: Small (< 50 employees)	**73.33%** 11	**26.67%** 4	**0.00%** 0	15
Q1: Medium (51 - 249 employees)	**100.00%** 3	**0.00%** 0	**0.00%** 0	3
Q1: Large (> 250 employees)	**45.61%** 26	**54.39%** 31	**0.00%** 0	57
Total Respondents	40	35	0	75

Figure 25. Traveller Tracking Comparison

Source: own work, Luzzi (2014)

In order to gain further insight in all the methods of traveller tracking used questionnaire respondents indicating the use of traveller tracking were asked, '*Which methods of traveller tracking are utilized?*' In response (Figure 26) the following use was indicated: reservation monitoring (56%); ticketing transactions (56%); technological monitoring (44%); other (18.67%) and 4% indicated they 'don't know'.

Q35 Which methods of traveller tracking are utilized?

Answered: 75

Answer Choices	Responses	
Reservation monitoring (ie. what is booked)	**56.00%**	42
Ticketing transactions monitoring (ie. what is actually executed)	**56.00%**	42
Technological monitoring (eg. mobile technology)	**44.00%**	33
Don't know	**4.00%**	3
Other (please specify)	**18.67%**	14

#	Other (please specify)	Date
1	iJET. Itineraries are tracked. Regional managers (like me) opt to receive alerts to the higher risk locations.	5/19/2014 10:01 AM
2	We use the Anvil system which links to our travel booking service. This allows us to see a comprehensive picture of all travellers in any location globally.	5/19/2014 9:23 AM
3	Telephone calls / emails	5/6/2014 12:51 AM
4	Anyone to high / extreme gets active tracking the rest via ticketing	4/24/2014 4:07 AM
5	Daily check-in	4/16/2014 2:26 AM
6	We use iJET. Itineraries are automatically loaded by the travel agent and Corporate Group has access to site to track, communicate with and send mass communications etc.	4/15/2014 1:13 PM
7	Track 24 gps	4/15/2014 11:38 AM
8	a combination of the above	4/15/2014 9:10 AM
9	The travel risk	4/15/2014 4:52 AM
10	Reservation monitoring unless high risk country and then GPS	4/15/2014 3:31 AM
11	Timed contact call back	4/15/2014 2:42 AM
12	Time based check in	4/15/2014 2:10 AM
13	checking in procedures, regular contact with HQ	4/15/2014 2:07 AM
14	red 24 travel tracker	4/15/2014 12:53 AM

Figure 26. Traveller Tracking Methods

Source: own work, Luzzi (2014)

From this it is evident that there is a significant use of technological monitoring. Due to the costs involved in this, it might be expected that it is mainly the large organisations that utilise this method of monitoring. However when filtering these results it can be seen that the majority of technological use is conducted by small organisations (80%), and the medium (66.67%) and larger organisations (33.33%) make more use of conventional monitoring methods of reservation and ticketing transaction monitoring.

P1 confirmed the use of a third party service provider to monitor employees. This however did not include the use of technological tracking. The interviewee highlighted that they are interested in using GPS tracking through a mobile device, but also outlined the legislative complexities in adopting such an approach:

Currently there are three ways you can track somebody. There is the itinerary based, which is a non-live based scenario where you are hoping that the person who says they are going to be in Shanghai didn't go to Beijing or somewhere where the bomb has gone off, and if they go off-piste you have no clue where they have gone. To the other extreme where you have GPS tracking, which is usually through a mobile device of some kind, a smart phone. But that would require full consent. It also breaches a number of laws, certainly European laws, such as French, Belgian and Holland. Privacy laws are very strict there on what you can and what you can't ask your employees to do, so there are huge legal implications of doing that, of mandating it.

P2 highlighted not using any travel tracking technology, instead making use of the conventional traveller monitoring methods:

No, we have no travel trackers or anything like that. Ijet allows you to monitor personnel. So we can log onto Ijet today and I can see exactly where people have travelled to globally, but in terms of real time tracking, there is nothing that we have got.

P3 confirmed the use of a technological product in conjunction with the conventional methods of monitoring. This mobile application however does not support traveller tracking. It is used as a tool for promulgation of travel risk, and the use of which is promoted, not mandatory. Privacy concerns were also highlighted as a reason for not utilising the technological tracking approach:

We haven't really considered it, or at least I haven't, certainly from the European arm of things. I would imagine in the US it's probably on privacy reasons why we don't do it, and again there are no real high risk locations involved.

Security Updates

In order to reduce the likelihood of an incident occurring or to reduce the impact of an incident, important and or updated security information needs to be relayed to travellers. This being to warn travellers of an imminent threat, deteriorating situation or recent incident. Questionnaire respondents were asked, '*Are business travellers supplied with important or updated security information during travel?*' In response 57.58% indicated 'yes', 34.85% indicated 'no' and 7.58% indicated they 'don't know' (Figure 27).

Q36 Are business travellers supplied with important or updated security information during travel?

Answered: 198

Answer Choices	Responses	
Yes	**57.58%**	114
No	**34.85%**	69
Don't know	**7.58%**	15
Total		**198**

Figure 27. Security Updates

Source: own work, Luzzi (2014)

These poor results are similar to those of Claus (2011a) who identified that 61% of respondents indicated their organisation keeps their travellers informed of changing risk conditions whilst travelling. Questionnaire respondents that indicated 'yes' to their organisation updating travellers were then asked, '*Is this provided for in-house or outsourced?*' In response 64.04% indicated 'in-house', 35.09% indicated 'outsourced' and 0.88% indicated they 'don't know' (Figure 28).

Q37 Is this provided for in-house or outsourced?

Answered: 114

Answer Choices	Responses	
In-house	**64.04%**	73
Outsourced	**35.09%**	40
Don't know	**0.88%**	1
Total		**114**

Figure 28. Responsibility for Traveller Security Updates

Source: own work, Luzzi (2014)

In order to establish which methods are used to update travellers, questionnaire respondents were asked, '*How is important security information provided to business travellers during travel?*'

In response 83.33% indicated email, 57.89% indicated text messages, 26.32% indicated intranet/website, 37.72% indicated mobile application and 19.30% indicated 'other' (Figure 29).

Q38 How is important security information provided to business travellers during travel?

Answered: 114

Answer Choices	Responses	
Email	**83.33%**	95
Text	**57.89%**	66
Intranet/website	**26.32%**	30
Mobile application	**37.72%**	43
Other (please specify)	**19.30%**	22

#	Other (please specify)	Date
1	Telephone	6/9/2014 7:58 AM
2	Combination of the above. Bulk text, email, voice etc.	5/19/2014 10:02 AM
3	The Anvil service can be set to user preference - email, text, call etc. It is also available online.	5/19/2014 9:24 AM
4	Siprnet scramble frequencies	5/15/2014 4:17 AM
5	mix of the above	5/14/2014 11:38 AM
6	Telephone calls	5/6/2014 12:51 AM
7	In the event it is a live incident we will call	4/24/2014 4:08 AM
8	Skype	4/18/2014 8:55 AM
9	Telephone Call in an emergency	4/16/2014 4:25 AM
10	verbal brief	4/16/2014 2:27 AM
11	voice over normal mobile networks, satellite phones etc.	4/16/2014 1:04 AM
12	Mass communications, procedures in place for locations to call travellers. Recent example, Tsunami Pacific Coast we used a combination of all. Predominantly iJET to confirm we had a number of foreign travellers in the location. Via iJET we reach out to all travellers by email and SMS with a tick box that they mark as being ok, or requiring assistance.	4/15/2014 1:15 PM
13	VOIP / Voice conversation	4/15/2014 11:08 AM
14	combination of the above	4/15/2014 9:10 AM
15	All of the above	4/15/2014 8:09 AM
16	Phone call	4/15/2014 3:38 AM
17	via Travel Agent and Company resources	4/15/2014 3:12 AM
18	Stopped at point of departure if security situation has deteriorated	4/15/2014 2:43 AM
19	Local staff	4/15/2014 2:42 AM
20	Call	4/15/2014 2:30 AM
21	Direct call to mobile/hotel	4/15/2014 2:29 AM
22	In-house analysts	4/15/2014 2:07 AM

Figure 29. Provision of Security Updates

Source: own work, Luzzi (2014)

All interviewees confirmed providing security updates. P1 highlighted this function being performed in-house and by their third party service providers, sending updated information via email. P2 confirmed these being provided by their third party service provider and well as being conducted ‘in-house’. The ‘in-house’ methods included using telephone calls, text messaging, email and the use of an Imodus (a secure web

based communication platform). P3 highlighted updates being provided through the third party service provider's mobile application.

Risk Transfer

Business travel insurance policies are used to transfer a portion of the associated risk. Advito (2009) advises that the person responsible for procurement of insurance is well aware of the travel risk management program as failure to understand the severity of the risk and complexity of the programme can result in inadequate cover for business travellers and potential liability for the traveller's organisation.

Crorie & Kawai (2014) suggest that one of the best ways for an organisation to minimise the risk of litigation is to ensure that kidnap and ransom insurance provides a high quality specialist response consultant service. Claus (2011a) highlights 35% of respondents indicated having employee kidnap and ransom insurance.

P1 alluded to the fact that senior management do not consider kidnap for ransom insurance necessary:

The executives don't think that they are that high profile enough for K & R, again that is probably a misconception but nevertheless they don't think they are.

P2 confirmed the use of general travel insurance but would not be drawn on the subject of kidnap and ransom insurance:

P2: All our employees have travel insurance, there may be other types of insurance that we shouldn't really talk about.

RL: Like kidnap and ransom, things like that?

P2: Yes. Possibly, there may be that type of insurance as well.

P3 confirmed without elaborating, to having general travel insurance as well as kidnap and ransom insurance in place for business travellers.

The obvious reluctance to discuss the measure is explained by DaSilva (2012). She explains that due to the extreme sensitivity of kidnapping, a firm condition of these policies is that their existence is never exposed to a third party or even all of the organisations personnel (it was for this reason that questionnaire respondents were not asked questions relating to specialist insurance products).

Evaluation

As with any risk management programme evaluation is a key aspect in order to determine and review programme effectiveness. Advito (2009) suggests several techniques for monitoring and ensuring the continuity of a travel risk management programme. These include creating a multi-disciplinary steering group, benchmarking regularly against best practices and peers, seeking input from senior managers on likely new destinations, collating traveller feedback on risk-related issues, reviewing policies and procedures when incidents happen and ensuring policy compliance remains high. McIndoe (2011) highlights that developing a comprehensive and proactive travel risk management programme is an ongoing responsibility that should be under continuous evaluation by identifying weaknesses and improvement by refocusing time and resources where needed.

Using questions based on the fundamental aspects of Kirkpatrick's learning and training evaluation theory (learning, reaction, behaviour and results), questionnaire respondents were asked several questions in order to determine how organisations assess and evaluate their countermeasures (Figure 30).

Q40 Does your organisation carry out any of the following procedures?

Answered: 197

	Yes	No	Don't know	Total
Pre-and post-travel security training testing	**27.41%** 54	**64.47%** 127	**8.12%** 16	197
Post trip debriefing/surveying of personnel in relation to training, planning, procedural and countermeasure effectiveness	**28.93%** 57	**61.93%** 122	**9.14%** 18	197
Interviews/observations to evaluate traveller behavior in relation to risk culture improvement	**18.78%** 37	**72.08%** 142	**9.14%** 18	197
Analysis of key performance indicators such as return on investment, incidents, staff retention, reputation and accreditation.	**27.41%** 54	**63.45%** 125	**9.14%** 18	197

Figure 30. Evaluation Procedures

Source: own work, Luzzi (2014)

These very poor results were put into perspective by the interviewees as they were also asked if the effectiveness of their travel security programme is evaluated and if so, how? P1 highlighted no evaluation apart from having conducted some test scenarios with their third party service provider to test the system in place:

I will be quite honest with you Rico I don't think it is evaluated, I mean the effectiveness of it is not evaluated. I guess the effectiveness of it is when something goes wrong, that's the evaluation. Did it work or did it not work.

The interviewee suggested that the main reason for not conducting a thorough evaluation of the effectiveness of the programme is more due to a lack of impetus and cohesiveness from top level executives, than it is the cost implications:

No it is a mind-set implication. I think to make it effective you have to prove that there is cost involved and that there's a grabbing back of costs in some ways. I think you have to prove that the return of investment is there and you have to get the mind-set of the people that have to do that as well, and as I said right at the beginning when you don't necessarily have the cohesive support, and I am not saying they are unsupportive, they are just a difficult forum to get all in one direction. Our head executives will have a lot of different opinions and then, you never end up with clear concise guidance. So actually if you don't have a proper system in place, then to evaluate the system we have is probably non-productive anyway. You need the proper cohesive system in place and then you can provide KPIs, then you can provide an evaluation of how effective that system has been.

P2 identified that travel security is examined as part of the internal audit of physical security. When asked if their organisation makes use of surveys or debriefing of personnel to identify incidents and problems the interviewee suggested having a reactive rather than proactive evaluation process:

No we don't do that proactively. We wouldn't necessarily contact someone who has just travelled somewhere and just say to them, how did it all go, is there anything we can improve? We wouldn't do that. If there was an incident then there would be that follow up and there would be an internal investigation and lessons learnt and everything like that, but in terms of being more proactive we don't do that.

P2 only identified obtaining feedback on the performance of the third party service providers, suggesting that further evaluation would be time consuming and also being unsure as to who the correct stakeholder would be to conduct an evaluation:

Yes I think time consuming especially and that comes down to resources then. And then I suppose who maybe should do it. Should we do it, or would it be a third party internally that would do it.

Similarly P3 highlighted having no formal evaluation of programme effectiveness apart from monitoring the performance of the third party service provider:

I am not aware of any evaluation, no, other than the performance of the third party. You know, do we think we are getting up to date information from them and are they providing a good service, but I am not aware of any full evaluation.

P3 when asked if interviews, observations or surveys are used to monitor and assess behaviour, identify issues and problems the interviewee only identified using informal discussions with frequent travellers:

I think we do that informally. It's something I have certainly been considering here in London primarily because of all the variety of various nationalities now resident and living, working in London, but then travelling all over the world but they are UK employees so therefore UK duty of care and all that, so it's something I have been considering, but at the moment it would be kind of informal where I would know who is travelling a lot for example, and I would just go and ask them how have you found the service that's provided, have you had to use them, what do you think of it, just informal stuff really.

In relation to training testing, P3 identified no testing of the awareness training that they provide to travelling personnel.

In order to determine how questionnaire respondents perceive the efficacy of their organisations management of travel security they were asked two very similar questions. The first question (Figure 31) being, '*How well do you consider your organisation plans, and provides, for personnel and executive protection in relation to any business travel?'*

Q9 How well do you consider your organisation plans, and provides, for personnel and executive protection in relation to any business travel?

Answered: 217

Answer Choices	Responses	
Very well	**35.48%**	77
Adequately	**45.16%**	98
Poorly	**17.51%**	38
Don't know	**1.84%**	4
Total		**217**

Figure 31. Initial Respondent Rating

Source: own work, Luzzi (2014)

The second question (Figure 32) being, '*Using a rating scale how effective would you rate your organisation is in relation to the management of security risks associated with business travel (where 1 is very poor and 10 is highly effective)?*'

Q43 Using a rating scale how effective would you rate your organisation is in relation to the management of security risks associated with business travel (where 1 is very poor and 10 is highly effective)?

Answered: 195

1	2	3	4	5	6	7	8	9	10	Total	Average Rating
6.15% 12	**5.64%** 11	**7.69%** 15	**9.23%** 18	**11.28%** 22	**6.67%** 13	**15.90%** 31	**18.97%** 37	**12.31%** 24	**6.15%** 12	195	6.09

Figure 32. Supplementary Respondent Rating

Source: own work, Luzzi (2014)

The first question was asked in the early stage of the questionnaire, and the second near the end of the questionnaire to determine if there would be a large scale fluctuation in perceived efficacy suggesting possible bias, however this was not the case. From the results of these two questions it is evident that a significant number of respondents indicate poor practice in relation to their organisations travel security risk management. This highlighting the need for a significant increase in the awareness of the security risk associated with business travel, and that many organisations are falling a long way short of effective risk management.

Chapter 5

Conclusion and Recommendations

Business travel is an important and commonly utilised modern business practice with failures regularly brought to the fore by the intensive scrutiny of the modern media. This research set out to determine the maturity of the practice by examining the core components of the travel security risk management process in both the strategic and operational contexts. In doing so the project discovered a gap in the literature as the literature review discovered there is limited academic literature on the security aspects related to the subject, and that which is available is predominantly provided by practitioners linked to commercial enterprise in the context of duty of care and/or corporate social responsibility.

In order to evaluate where travel security risk management currently stands in terms of maturity, the research project methodically analysed the core components of the practice by asking five fundamental questions:

Who are the stakeholders involved in the practice?

How is this risk being assessed?

How is the risk being promulgated to personnel?

How is it being managed?

How are travel risk management programmes being evaluated?

The findings of the research were achieved using a mixed methods approach. Quantatively this took the form of a survey using an online questionnaire distributed to recognised security and human resource professionals as well as business leaders. Qualitative data was produced by conducting semi-structured interviews with

representatives responsible for the practice employed in three large multi-national organisations. Then by using triangulation, data generated from these two forms of analysis were synthesised with the data and theory discovered in the literature review, to reveal the research findings. This in turn enabling a judgement and recommendations to be made.

Stakeholder involvement in business travel is very much dependant on the contextual influence of an organisation's size, industry and operating location. Several business departments were highlighted having a significant role in the practice. These being senior management and security, human resource, risk management, operations, health and safety, and travel management departments. In terms of specific functions, security departments are predominantly responsible for policy creation, risk ownership and incident management. Senior management feature highly in responsibility for pre-trip authorisation.

Herein however lies a problem as the literature identifies senior management, who have only a medium level of security awareness, making security related decisions. This compounds another problem in that senior management are also predominantly responsible for programme initiation. In strategic terms the results commonly identified that there is a fifty-fifty share of responsibility between the traveller and the organisation. This may be due to organisations feeling that their personnel have a responsibility to take every possible precaution and to adhere to prescribed policies and procedures, and travellers feeling that they are in harm's way and deserve to be protected whilst on official business.

Strategically risk assessment involves consideration when expanding operations or deploying personnel on long term assignment. Operationally it is required prior to each and every trip, as well as being part of a continuous monitoring function. Risk assessment is predominantly conducted by 'in-house' personnel as well as being outsourced to specialist third party service providers. This may be due to the fact that there is a large amount of freely available information and outsourcing the function for

large organisations with many travellers can be costly. The results highlight significant use of specialist third party service providers. A reason for this may be due to organisations not having the dedicated departments to conduct travel security risk assessments.

Promulgation of the security risk associated with business travel requires the development and implementation of a comprehensive travel security policy which highlights a specific risk owner, and encompasses a compulsory pre-trip authorisation procedure, a compulsory booking procedure, a pre-trip advisory procedure and security specific training. The literature and results indicate that a significant number of organisations do not have a dedicated travel security policy, that there is a low level of inclusion of business travel security risks in other policies. This may be due to two reasons. Firstly, business travel may be considered to be a resulting action (of globalisation and the expansion of operations), and not a business process requiring strategic planning. Secondly, there is no defined level of accountability in relation to responsibility for travel security risk management, ie. organisation versus traveller.

The research indicates poor usage of security specific training in organisations. That which is done, is predominantly carried out by 'in-house' personnel. Training however must not only be seen as a countermeasure for business travellers. It is important that the stakeholders involved in the management of the risk, which includes those responsible for the procurement of insurance products and third party service providers, emergency response and crisis management teams, are all well trained in the execution of their duties and areas of responsibility. The degree and extent to which training is conducted should be based on the results of risk assessment taking into account contextual influences such as an organisation's operating location, industry type, length of deployment and identity/reputation. The poor implementation of training may be due to the low levels or lack of awareness in travel security risk by top level management, the failure to identify and evaluate the effect training can have, or misguided return of investment calculations.

In terms of managing the risk there are several approaches to consider. The first being risk avoidance which relates strategically to the consideration not to travel to a particular location based on risk appetite, the suspension of travel to a particular location in response to changes in risk level, and restrictions on the number of key personnel that can travel together. The research highlights that for this method of risk management to be effective a robust compulsory pre-trip authorisation procedures must be in place based on the results of an up to date risk assessment.

The second risk management approach is risk transfer. In relation to business travel this involves the use of comprehensive business insurance products and specialist insurance such as kidnap and ransom insurance. The research highlights the importance of an effective pre-trip authorisation procedure to be in place to ensure that personnel are provided with the required level of insurance cover prior to travel, as well as access to specialist consultants prior to departure. As well as ensuring that the person responsible for the procurement of these products is a key stakeholder in the management of this risk.

The third risk management approach is that of risk reduction. This entails the provision of an emergency contact point as part of an emergency or crisis response plan. The results indicate high usage of this practice being predominantly managed by 'in-house' personnel. The research reveals that for this measure to be effective the pre-trip advisory must ensure travellers have all the necessary contact and protocol information as well as a travel convenient plastic emergency contact card. Importantly this must be formally acknowledged by the traveller, and training must be provided to ensure all key emergency response stakeholders are rehearsed in their role.

Traveller tracking is another risk reduction countermeasure which can be carried out proactively or used as a response tool using three methods. These being the use of itinerary (planned), expense (paid for), or technological (real-time) data. The results indicate that there is only a medium to low level use of active traveller tracking, which is being conducted on near equal levels in-house and by outsourcing. The research

reveals that variations in levels of the use outsourcing are mainly affected by organisational size, and that large organisations are predominantly using conventional tracking methods instead of technological tracking which may be associated to costs and the complexity of privacy concerns across international boundaries. These poor results are important as not being able to quickly locate travellers in the event of an incident can inhibit emergency response measures, moreover an opportunity may be missed to forewarn travellers of an imminent threat.

The last risk reduction countermeasure explored was that of providing security updates to travellers. The results indicate only a medium level use of this countermeasure, and being predominantly carried out 'in-house'. The failure of an organisation to provide updated security information to its travellers can undermine the efforts of a travel risk management program, as a lack of proactivity renders response the only option. For this countermeasure to be effective it is also vital that the business traveller is provided with the necessary communication equipment, and training in its use.

The final aspect of the research examined how organisations evaluate the effectiveness of their travel risk management programme. This is a critical aspect of any risk management program as it enables the identification of strengths and weaknesses to guide further development. It entails testing trainees before and after training to determine its efficacy, surveying or debriefing travellers after travel to identify areas of improvement, conducting interviews or observations to determine if there is a change in risk culture, and analysis of key performance indicators to provide stakeholders with actionable metrics to evaluate and increase programme efficacy. The research results indicate low usage of these methods suggesting an ad hoc and fragmented approach to managing the risk which may be caused by a lack of awareness and poor risk oversight.

In examining each of the specified research questions the research project has provided a methodical and thorough inspection of the core components required for a travel risk management programme to determine their nature and condition of use. However this project, being an empirical study, is not without limitations. The qualitative data cannot

be considered truly generalizable due to the sample size. Inequalities in the sample sub-group sizes may also underestimate the extent of poor practice. This is due to the fact that the research sample group consists of a significantly larger amount of security practitioners providing feedback on a security related topic, possibly indicating better use of the practice than if there was a low level or no security practitioners in the sample group. This limitation however does not detract from the findings of the research, it actually reinforces the results. To rectify this limitation future research sample groups should include a similar number of human resource practitioners and business leaders as not all organisations have dedicated security departments.

With more and more personnel travelling for business and the increasing intensity and scrutiny of failures in travel risk management by government, legal entities and the media, which includes the advent of social media, one would assume that modern day organisations would be paying significant attention to the security risk involved with business travel. On the contrary, the results of this research suggest that business travel security risk management is generally only at a 'defined' level.

In order to facilitate and progress the general maturity of travel security risk management, the design and development of a business travel security standard, through the British Standards Institute, is recommended (currently being implemented by the researcher). There are standards in use which have principles that can be related to the practice and are transferable, such as British Standard BS EN ISO 22301:2014, however a standard specific to the practice, is recommended. This would guide organisations of any size, especially those without dedicated security departments (who should be considered the preferred risk owners), and in any industry in designing, implementing and managing a travel security risk management programme. This in turn could be beneficial to an organisation as it may attract key personnel, improve productivity and well-being in the workplace, and improve their reputation due to a positive corporate social responsibility image. A standard, which if adopted by the insurance industry, could possibly reduce the premiums for travel and specialist insurance products. It could also assist with regulatory and legal aspects in terms of criminal liability claims by providing a benchmark in terms of the ALARP principle. The descriptive nature of a

standard may also improve the quality of service received from third party service providers, as organisations will have a clear understanding of what to expect from them. The benefits deriving from the implementation of a standard would go a long way to improve the general level of travel security risk management towards an 'optimised' level.

Word Count: 21922 (excluding tables and figures)

Bibliography

Advito. (2007). *Responsible Travel Management*, [Online]. Available at: http://www.advito.com/aw/home/Global_website/en-us/Content/Resource_Center/~bmk/White_Papers/ [accessed 21 March 2013]

Advito (2009). *"C'est la vie?" a step-by-step guide to building a travel risk management program*, [Online]. Available at: http://www.advito.com/solutions/wp-link-travel-risk-mgmt/ [accessed 27 February 2013]

Aguilera, A. (2008). Business travel and mobile workers. *Transportation Research Part A*, [Online]. 42 (8), 1109-1116. Available at: http://www.sciencedirect.com/science/journal/09658564/42/8 [accessed 21 March 2013]

AIRMIC, ALARM & IRM. (2002). *A Risk Management Standard*, [Online]. Available at: http://www.theirm.org/publications/documents/Risk_Management_Standard_030820.pdf [accessed 21 March 2013]

AIG (2011). *AIG White Paper: pre-travel risk assessment*, [Online]. Available at: http://www.aig.co.uk/chartis/internet/uk/eni/AI426416-LP-White-Paper-12-12-Web_tcm2538-447497.pdf [accessed 15 September 2014]

Ball, D. & Machin, N. (2006). Foreign travel and the risk of harm. *International Journal of Injury Control and Safety Promotion*, [Online]. 13 (2), 107-115. Available at: http://www.tandfonline.com [accessed 21 March 2013]

Bates, R. (2004). A critical analysis of evaluation practice: the Kirkpatrick model and the principle of beneficence. *Evaluation and Program Learning*, [Online]. 27 (3), 341-347. Available at: http://www.sciencedirect.com/science/article/pii/S0149718904000369# [accessed 15 September 2014]

Beaverstock, J. et al. (2009). International Business Travel: some explorations. *Geografiska Annaler: Series B, Human Geography*, [Online]. 91 (3), 193-202. Available at: http://onlinelibrary.wiley.com/journal/10.1111/%28ISSN%291468-0467 [accessed 24 March 2013]

Biersdorff, K. (2009). *How many is enough? The quest for an acceptable survey response rate*, [Online]. Available at: http://kkbiersdorff.wordpress.com/2009/09/16/how-many-is-enough/ [accessed 23 November 2014]

Blaxter, L. & Hughes, C. & Tight, M. (2006). *How to Research* (3rd ed.). Maidenhead, UK: Open University Press

Borodzicz, E.P. (2005). *Risk, Crisis & Security Management*. Chichester, UK: John Wiley & Sons Ltd

Brereton, P. & Kitchenham, B. & Budgen, D. & Li, Z. (2008). *Using a Protocol Template for Case Study Planning*. [Online]. Available at: http://ewic.bcs.org/content/ConWebDoc/19535 [accessed 07 June 2013]

British Standards Institution. (2011). *BS 31100:2011. Risk Management – Code of practice and guidance for the implementation of BS ISO 31100.* London: British Standards Institution

British Standards Institution. (2014). *BS EN ISO 22301:2014. Societal Security – Business continuity management systems – Requirements (ISO 22301:2012)*. London: British Standards Institution

Brodeur, A. & Buehler, K. & Patsalos-Fox, M. & Pergler, M. (2010). *McKinsey Working Papers on Risk, Number 18: a board perspective on enterprise risk management*, [Online]. Available at: http://www.mckinsey.com/client_service/risk/latest_thinking/working_papers_on_risk [accessed 21 March 2013]

Brodeur, A. & Pergler, M. (2010). *McKinsey Working Papers on Risk, Number 22: top-down ERM: a pragmatic approach to managing risk from the C-suite*, [Online]. Available at: http://www.mckinsey.com/client_service/risk/latest_thinking/working_papers_on_risk [accessed 21 March 2013]

Brooks, D. (2011). Security risk management: a psychometric map of expert knowledge structure. *Risk Management*, [Online]. 13 (1/2), 17-41. Available at: http://www.palgrave-journals.com/rm/index.html [accessed 17 March 2013]

Claus, L. (2011a). *Duty of Care and Travel Risk Management Global Benchmarking Study*, [Online]. Available at: http://www.internationalsosfoundation.org/resources/white-papers/ [accessed 27 February 2013]

Claus, L. (2011b). *Duty of Care and Travel Risk Management Benchmarking Study Europe*, [Online]. Available at: http://www.internationalsosfoundation.org/resources/white-papers/ [accessed 27 February 2013]

Cousins, F. (2010). Protect & Defend. *Business Traveller (UK/Europe Edition)*, [Online]. April 2010, 28-30. Available at: http://search.ebscohost.com/ (Business Source Complete) [accessed 21 May 2011]

Crittenden, P. (2012). The Dollars & Sense of Business Travel Security Awareness. *Security: Solutions for Enterprise Security Leaders*, [Online]. 49 (9), 38-42. Available at: http://search.ebscohost.com/ (Business Source Complete) [accessed 21 March 2013]

Crorie, M. & Kawai, E. (2014). *Kidnap and the liability of businesses*, [Online]. Available at: http://www.clydeco.com/uploads/Files/CC005339_Kidnap_liability_of_business_Update_09_06_14_final.pdf [accessed 10 June 2014]

Da Silva, A. (2014). *Kidnapping for ransom and extortion on increase in emerging markets*, [Online]. Available at: http://itinews.co.za/companyview.aspx?cocategoryid=61&companyid=22416&itemid=1A9BAC93-FE6B-4DA0-889C-62584C41AA13 [accessed 13 June 2014]

Davidson, M. (2009). *Managing Risk Across the Enterprise*, [Online]. Available at: http://www.securitymanagement.com/magazine/2009/07 [accessed 17 March 2013]

Deroose, P. (2013). *How to Prepare for an Evacuation*, [Online]. Available at: http://www.securitymagazine.com/articles/print/84187-how-to-prepare-for-an-evacuation?goback=.gde_3936559_member_229553962 [accessed 14 May 2013]

Donnelly, R. et al. (2012). Redesigning risk framework and registers to support the assessment and communication of risk in the corporate context: lessons from a corporate risk manager in action. *Risk Management*, [Online]. 14 (3), 222-247. Available at: http://www.palgrave-journals.com/rm/index.html [accessed 17 March 2013]

Douglas, A. & Lubbe, B. (2010). An Empirical Investigation into the Role of Personal-Related Factors on Corporate Travel Policy Compliance. *Journal of Business Ethics*, [Online]. 92 (3), 451-461. Available at: http://search.ebscohost.com/ (Business Source Complete) [accessed 14 March 2013]

Dudko-Richardson, E. (2014). *Are you being Hacked on Your Business Travels around the world*? [Online]. Available at: https://biztobiztv.wordpress.com/2014/11/12/are-you-being-hacked-on-your-business-travels-around-the-world/ [accessed 22 November 2014]

Eisenhardt, K. (1989). Building Theories from Case Study Research. *The Academy of Management Review*, [Online]. 14 (4), 532-550. Available at: http://www.jstor.org/action/showPublication?journalCode=acadmanarevi [accessed 07 June 2013]

Evans, J. & Mathur, A. (2005). The value of online surveys. *Internet Research*, [Online]. 15 (2), 195-219. Available at: www.emeraldinsight.com/journals.htm?issn=1066-2243 [accessed 14 June 2013]

Fricker, R. & Schonlau, M. (2002). Advantages and Disadvantages of Internet Research Surveys: evidence from the Literature. *Field Methods*, [Online]. 14 (4), 347-367. Available at: http://fmx.sagepub.com/ [accessed 07 June 2013]

Giangreco, A. & Carugati, A. & Sebastiano, A. (2010). Are we doing the right thing?: food for thought on training evaluation and its context. *Personnel Review,* [Online]. 39 (2), 162-177. Available at: http://www.emeraldinsight.com/doi/abs/10.1108/00483481011017390 [accessed 15 September 2014]

Gibb, F. & Buchanan, S. (2006). A framework for business continuity management. *International Journal of Information Management*, [Online]. 26 (2), 128-141. Available at: http://www.sciencedirect.com/science/journal/02684012 [accessed 5 March 2014]

Glab, J. (2012). *Corporate Travel Safety,* [Online]. Available at: http://www.executivetravelmagazine.com/articles/corporate-travel-safety [accessed 12 March 2014]

Health and Safety Executive. (2013). *Corporate Manslaughter*, [Online]. Available at: http://www.hse.gov.uk/corpmanslaughter/ [accessed 23 December 2013]

Health and Safety Executive. (2014). *ALARP,* [Online]. Available at: http://www.hse.gov.uk/risk/theory/alarpglance.htm [accessed 09 November 2014]

Hearnden, K. & Moore, A. (1999). *The Handbook of Business Security: a practical guide to managing the security risk*. London, UK: Kogan Page Ltd

Hiles, A. ed. (2007). *The Definitive Handbook of Business Continuity Management* (2nd ed.). Chichester, UK: John Wiley & Sons Ltd

Hopkin, P. (2010). *Fundamentals of Risk Management: understanding, evaluating and implementing effective risk management.* London, UK: The Institute of Risk Management

HRFocus. (2008). Protect Employees and Information With a Business Travel Security Policy. *HRFocus*, [Online]. 85 (1), 5-6. Available at: http://search.ebscohost.com/ (Business Source Complete) [accessed 12 March 2013]

Hubbard, D.W. (2009). *The Failure of Risk Management: why it's broken and how to fix it*. New Jersey, USA: John Wiley & Sons Ltd

International SOS (2011). *International SOS survey reveals business travellers in high-risk destinations value location-specific alerts and travel-tracking capability*, [Online]. Available at: https://www.internationalsos.com/en/pressreleases_5792.htm [accessed 14 March 2014]

Jonas, D. (2012). *Survey: Travel Risk Management Practices Becoming More Prevalent*, [Online]. Available at: http://www.businesstravelnews.com/Travel-Management/Survey--Travel-Risk-Management-Practices-Becoming-More-Prevalent/?a=mgmt [accessed 12 March 2013]

Krivkovich, A. & Levy, C. (2013). *Managing the people side of risk*, [Online]. Available at: http://www.mckinsey.com/insights/risk_management/managing_the_people_side_of_risk [accessed 13 May 2013]

Kumar, R. (2005). *Research Methodology: a step-by-step guide for beginners* (2nd ed.). London, UK: SAGE Publications Ltd

Lalonde, C. & Boiral, O. (2012). Managing risks through ISO 31000: a critical analysis. *Risk Management*, [Online]. 14 (4), 272-300. Available at: http://www.palgrave-journals.com/rm/index.html [accessed 21 March 2013]

Layak, S. & Madhavan, N. & Sachitanand, R. (2011). Ready For Doomsday? *Business Today*, [Online]. 20 (9) 52-56. Available at: http://search.ebscohost.com/ (Business Source Complete) [accessed 21 March 2013]

Leedy, P. & Ormrod, E. (2010). *Practical Research: planning and design* (9th ed.). New Jersey, USA: Pearson Education International

Lippert, R. & Walby, K. & Steckle, R. (2013). Multiplicities of corporate security: identifying emerging types, trends and issues. *Security Journal*, [Online]. 26 (3), 206-221. Available at: http://www.palgrave-journals.com/sj/journal/v26/n3/full/sj201312a.html [accessed 17 February 2014]

Longmore-Etheridge, A. (n.d). *The Risky Business of Travel*, [Online]. Available at: http://securitymanagement.com/article/risky-business-travel-0012461 [accessed 04 April 2014]

Mahesh, N. & Morash, M. (2002). Assessing the Scope of Corporate Security: common practices and relationships with other business functions. *Security Journal*, [Online]. 15 (3), 7-19. Available at: http://www.palgrave-journals.com/sj/index.html [accessed 21 March 2013]

McGill, W. & Ayyub, B. & Kaminskiy, M. (2007). Risk Analysis for Critical Asset Protection. *Risk Analysis*, [Online]. 27 (5), 1265-1281. Available at: http://onlinelibrary.wiley.com/journal/10.1111/%28ISSN%291539-6924 [accessed 7 March 2013]

McIndoe, B. (2011). How To Design And Deploy An Effective Travel Risk Management Program. *Business Travel News*, [Online]. 28 (1), 30-30. Available at: http://search.ebscohost.com/ (Business Source Complete) [accessed 21 March 2013]

McNulty, M. (2013). *Travel Often Part Of Multi-Disciplined Risk Management Approach*, [Online]. Available at: http://www.businesstravelnews.com/Travel-Management/Travel-Often-Part-Of-Multi-Disciplined-Risk-Management-Approach/?a=btn [accessed 12 March 2013]

Mullins, L. J. & Christy, G. (2010). *Management & Organisational Behaviour*. 9th ed. Harlow, UK: Financial Times, Prentice Hall.

Neill, J. (2007). *Qualitative versus Quantitative Research: key points in a classic debate*. [Online]. Available at: http://wilderdom.com/research/QualitativeVersusQuantitativeResearch.html [accessed 07 June 2013]

Office for National Statistics (2014). *Travel Trends 2013: key findings*, [Online]. Available at: http://www.ons.gov.uk/ons/rel/ott/travel-trends/2013/rpt-travel-trends--2013.html [accessed 23 October 2014]

O'Reilly, C. (2011). "From Kidnaps to Contagious Diseases": elite rescue and the strategic expansion of the transnational security consultancy industry. *International Political Sociology*, [Online]. 5 (2), 178-197. Available at: http://onlinelibrary.wiley.com/journal/10.1111/%28ISSN%291749-5687 [accessed 21 March 2013]

Rabiee, F. (2004). Focus-group interview and data analysis. *Proceedings of the Nutrition Society*, [Online]. 63 (4), 655-660. Available at: http://journals.cambridge.org/action/displayJournal?jid=PNS [accessed 07 June 2013]

Rahim, M. (2011). *Managing Conflict in Organisations* (4th ed.). New Jersey, USA: Transaction Publishers

Rendeiro, J. (2012). Duty of Care: what's the security director's role? *Security: Solutions for Enterprise Security Leaders*, [Online]. 49 (3), 38-40. Available at: http://search.ebscohost.com/ (Business Source Complete) [accessed 21 March 2013]

Rendeiro, J. (2013). Threat Analysis and Ratings for the Security Manager: the broad view. *Security: Solutions for Enterprise Security Leaders*, [Online]. 50 (1), 22-26. Available at: http://search.ebscohost.com/ (Business Source Complete) [accessed 12 March 2013]

Reuvid, J. ed. (2008). *Managing Business Risk: a practical guide to protecting your business* (5th ed.). London, UK: Kogan Page Limited

Ritchey, D. (2012). *Managing Risk on the Global Stage*, [online]. Available at: http://www.securitymagazine.com/articles/83447-managing-risk-on-the-global-stage [accessed 14 March 2013]

Saunders, M. & Lewis, P. & Thornhill, A. (2012). *Research Methods for Business Students* (6th ed.). Harlow, UK: Pearson Education Limited

Schneier, B. (2008). *The Psychology of Security*, [Online]. Available at: http://www.schneier.com/paper-psychology-of-security.html [accessed 07 June 2013]

Simpson, P. & Siguaw, J. (2008). Perceived Travel Risks: the traveller perspective and manageability. *International Journal of Tourism Research*, [Online]. 10 (4), 315-327. Available at: http://onlinelibrary.wiley.com/journal/10.1002/%28ISSN%291522-1970 [accessed 21 March 2013]

Smith, D. & Fischbacher, M. (2009). The changing nature of risk and risk management: The challenge of borders, uncertainty and resilience. *Risk Management*, [Online]. 11 (1), 1-12. Available at: http://www.palgrave-journals.com/rm/index.html [accessed 13 March 2013]

Society for Human Resource Management (2009). *Many Firms Limit Number of Executives on Same Flight*, [Online]. Available at: http://www.shrm.org/publications/hrnews/pages/limitnumbersameflight.aspx [accessed 29 August 2014]

Strom, K. et al. (2010). *The Private Security Industry: a review of the definitions, available data sources, and paths moving forward*, [Online]. Available at: https://www.ncjrs.gov/pdffiles1/bjs/grants/232781.pdf [accessed 05 June 2014]

Talbot, J. & Jakeman, M. (2009). *Security Risk Management: body of knowledge*. New Jersey, USA: John Wiley & Sons, Inc.

Torma-Krajewski, J. & Powers, J. (2010). *Decision-Making and Emergency Responses: training for incident command centres and mine rescue teams*, [Online]. Available at: http://inside.mines.edu/UserFiles/File/MSHP/Decision-Making%20Training%20Manual%20-%20Final%20-%20Updated.pdf [accessed 15 November 2014]

University of Strathclyde (2013). *What is observation?*, [Online]. Available at: http://www.strath.ac.uk/aer/materials/3datacollection/unit5/whatisobservation/ [accessed 07 June 2013]

Walby, K. & Lippert, R. (2014). Introduction: governing every person, place, and thing – critical studies of corporate security. In K. Walby & R. Lippert, eds. *Corporate Security In The 21st Century: theory and practice in international perspective*. Hampshire, UK: Macmillan Publishers Limited

Walliman, N. (2011). *Your Research Project: designing and planning your work* (3rd ed.). London, UK: SAGE Publications Ltd

Ward, S. (2003). Approaches to Integrated Risk Management: a multi-dimensional framework. *Risk Management*, [Online]. 5 (4), 7-23. Available at: http://www.palgrave-journals.com/rm/index.html [accessed 17 March 2013]

Wilding, E. (2009). *Information Risk and Security: preventing and investigating workplace computer crime*. Farnham, UK: Ashgate Publishing Limited (Original work published 2006)

Wirz, M. (2012). *Travel Advisories: qualitative analysis of foreign office advisories and prototyping a new generation of advisories*. MSc. Dissertation. Cologne University of Applied Sciences

Wojcik, J. (2012). Managing foreign travel risks. *Business Insurance*, [Online]. 46 (39), 6-6. Available at: http://search.ebscohost.com/ (Business Source Complete) [accessed 21 March 2013]

Wright, K. (2005). Researching Internet-based populations: advantages and disadvantages of online survey research, online questionnaire authoring software packages, and web survey services. *Journal of Computer-Mediated Communication,* [Online]. 10 (3), article 11. Available at: www.onlinelibrary.wiley.com/journal/10.1111/%28ISSN%291083-6101 [accessed 13 June 2013]

Yin, R. (2009). *Case Study Research: design and methods* (4th ed.). London, UK: SAGE Ltd

Zucker, D. (2009). *How to Do Case Study Research*, [Online]. Available at: http://scholarworks.umass.edu/nursing_faculty_pubs/ [accessed 07 June 2013]

Zurich (2012). *Honoring your Duty of Care for employees in high-risk areas*, [Online]. Available at: http://www.zurichna.com/internet/zna/sitecollectiondocuments/en/products/accidentandhealth/duty%20of%20care%20wp.pdf [accessed 25 July 2014]

Appendices

Appendix 1. Advito High Risk Area Advice

Appendix 2. Online Questionnaire

Appendix 3. Questionnaire Formal Request for Assistance

Appendix 4. Supplementary Questionnaire Formal Request for Assistance

Appendix 5. Questionnaire Introduction

Appendix 6. Interview Template

Appendix 7. Interview Request

Appendix 8. Transcription Interview One

Appendix 9. Transcription Interview Two

Appendix 10. Transcription Interview Three

Appendix 1.

Advito High Risk Area Advice

Travel to hot spots

Take off all company tags, logos, etc., from luggage and clothes.

Make reservations through your global travel agency. They have been instructed to remove the company name from all tickets and itineraries.

Use a charge card that is not branded with the company name or use a personal credit card.

When registering in a hotel, use only your name, not the company's name.

Do not identify your company to immigration or customs officials.

Note on immigration forms that the purpose of your visit is to attend a conference – not specified.

Inform only your family and one or two colleagues of the details of your travel.

In politically unstable countries, you should register your name and passport number with your Embassy. Passports should be kept secure at all times.

Avoid leaving the hotel at the same time and following the same route every day.

Source: Advito (2009, p.31)

Appendix 2.

Online Questionnaire

Q1 What is the size of your organisation?

Answered: 218

Answer Choices	Responses	
Small (< 50 employees)	**21.56%**	47
Medium (51 - 249 employees)	**6.42%**	14
Large (> 250 employees)	**71.56%**	156
Don't know	**0.46%**	1
Total		**218**

Q2 Is your organisation multinational?

Answered: 218

Answer Choices	Responses	
Yes	**71.10%**	155
No	**28.44%**	62
Don't know	**0.46%**	1
Total		**218**

Q3 Are the headquarters of your organisation in the United Kingdom?

Answered: 218

Answer Choices	Responses	
Yes	**59.63%**	130
No	**39.45%**	86
Don't know	**0.00%**	0
Not applicable	**0.92%**	2
Total		**218**

Q4 In which industry does your organisation operate?

Answered: 218

Answer Choices	Responses	
Aerospace	**2.29%**	5
Asset management	**0.92%**	2
Automotive	**0.46%**	1
Education	**11.47%**	25
Communications & technology	**4.13%**	9
Chemicals	**0.92%**	2
Construction & real estate	**1.38%**	3
Defence & security	**14.22%**	31
Energy, utilities & mining	**11.01%**	24
Manufacturing	**5.50%**	12
Entertainment & media	**0.92%**	2
Financial services & insurance	**11.93%**	26
Government & public services	**9.17%**	20
Healthcare & pharmaceuticals	**5.96%**	13
Retail, hospitality & leisure	**2.29%**	5
Transportation & logistics	**2.29%**	5
Other (please specify)	**15.14%**	33
Total		**218**

#	Other (please specify)	Date
1	Water and Environment - Engineering	6/18/2014 8:42 AM
2	security training and consultancy services	6/9/2014 8:32 PM
3	Charity	6/9/2014 7:11 AM
4	Consulting	6/9/2014 4:32 AM
5	International Organization	5/26/2014 4:53 AM
6	Accounting	5/20/2014 2:26 PM
7	IT & Software	5/15/2014 4:54 AM
8	Services and BPO	5/14/2014 5:16 AM
9	highways, Rail, Utilities	5/12/2014 1:34 AM
10	Commercial Airline	5/7/2014 11:36 AM

11	Humanitarian Assistance	5/6/2014 12:47 AM
12	Software, Devices & Services	5/5/2014 9:17 AM
13	Not for profit - business services	4/28/2014 8:13 AM
14	Research and education in the built environment	4/22/2014 4:58 AM
15	General commercial	4/18/2014 8:50 AM
16	Higher Education	4/17/2014 1:51 AM
17	All of the above as we area facilities and security provider	4/16/2014 3:35 AM
18	market research	4/16/2014 3:17 AM
19	Digital media and marketing	4/16/2014 1:43 AM
20	I cover a number of industries on the above list	4/15/2014 10:11 PM
21	Consultancy	4/15/2014 1:26 PM
22	Information/IT Security	4/15/2014 12:07 PM
23	Engineering Consultancy	4/15/2014 11:18 AM
24	Consultancy and Training	4/15/2014 8:56 AM
25	Global Facilities Management and constructions services	4/15/2014 8:43 AM
26	Oil & Gas	4/15/2014 8:42 AM
27	Agribusiness	4/15/2014 8:34 AM
28	NGO	4/15/2014 8:30 AM
29	United Nations	4/15/2014 2:37 AM
30	Oil and Gas	4/15/2014 2:36 AM
31	security & justice	4/15/2014 2:03 AM
32	Risk consultancy	4/15/2014 2:02 AM
33	Research and Higher Education	4/15/2014 12:48 AM

Q5 Which of the following best describes the level at which you operate in the organisation?

Answered: 218

Answer Choices	Responses	
Top-level (director/chairman)	**14.68%**	32
Senior-level (C-level)	**20.64%**	45
Middle-level (senior manager)	**39.45%**	86
Supervisory (manager)	**19.27%**	42
Contributor or operative	**5.96%**	13
Don't know	**0.00%**	0
Total		**218**

Q6 Which department do you belong to?

Answered: 218

Answer Choices	Responses	
Top-level management	**12.84%**	28
Human resources	**5.96%**	13
Security	**49.54%**	108
Risk management	**7.80%**	17
Legal	**0.92%**	2
Health, safety & environment	**2.29%**	5
Travel management	**0.46%**	1
Operations	**9.63%**	21
Other (please specify)	**10.55%**	23
Total		**218**

#	Other (please specify)	Date
1	Consultants Group	6/12/2014 12:44 AM
2	Finance	6/9/2014 7:22 AM
3	Commercial	6/9/2014 3:07 AM
4	company owner	5/21/2014 3:35 AM
5	Responsibility for Security, Crisis Response and Travel Risk	5/19/2014 9:54 AM
6	regional marketing	5/17/2014 4:02 AM
7	Finance	5/14/2014 5:16 AM
8	Safety and risk and operations	5/7/2014 11:37 AM
9	Business development (+Tutor and Assessor)	5/7/2014 7:22 AM
10	Project manager for electronic security assessment services	4/22/2014 4:59 AM
11	Business Continuity and Security	4/16/2014 2:16 AM
12	Safety and Security	4/16/2014 1:44 AM
13	Crisis and Emergency Management, Security and Travel Risk	4/15/2014 1:01 PM
14	Specialist Consultancy	4/15/2014 11:19 AM
15	Operational Development	4/15/2014 7:51 AM
16	Research and Education	4/15/2014 7:25 AM
17	Compliance	4/15/2014 4:55 AM
18	Consultant	4/15/2014 3:36 AM
19	central support services incl. security	4/14/2014 3:20 AM
20	Estates	4/14/2014 2:54 AM

21	Estates	4/14/2014 1:21 AM
22	Facilities	4/14/2014 1:18 AM
23	HSSE	4/14/2014 1:04 AM

Q7 Does your organisation have the following dedicated departments?

Answered: 218

	Yes	No	Don't know	Total
Human resources	**87.61%** 191	**12.39%** 27	**0.00%** 0	218
Security	**80.28%** 175	**18.35%** 40	**1.38%** 3	218
Risk management	**70.18%** 153	**27.98%** 61	**1.83%** 4	218
Legal	**73.85%** 161	**26.15%** 57	**0.00%** 0	218
Health, safety & environment	**76.15%** 166	**22.94%** 50	**0.92%** 2	218
Travel management	**52.75%** 115	**45.41%** 99	**1.83%** 4	218
Operations	**84.40%** 184	**14.22%** 31	**1.38%** 3	218

Q8 Are you, your co-workers or executives required to travel as part of your employment?

Answered: 218

Answer Choices	Responses	
Yes	**100.00%**	218
No	**0.00%**	0
Total		**218**

Q9 How well do you consider your organisation plans, and provides, for personnel and executive protection in relation to any business travel?

Answered: 217

Answer Choices	Responses	
Very well	**35.48%**	77
Adequately	**45.16%**	98
Poorly	**17.51%**	38
Don't know	**1.84%**	4
Total		**217**

Q10 Are you well aware of the legal responsibilities and requirements placed upon an employer to ensure the Duty of Care of its personnel?

Answered: 211

Answer Choices	Responses	
Yes	**86.73%**	183
No	**13.27%**	28
Total		**211**

Q11 Who do you consider SHOULD be responsible for the management of security related risk when travelling for business?

Answered: 211

Travellers sole responsibility	Travellers responsibility with organisational support	Equal responsibility	Mainly organisations responsibility with travellers input	Organisations sole responsibility	Total
0.95%	**16.11%**	**37.44%**	**39.34%**	**6.16%**	
2	34	79	83	13	211

Q12 Do you have a formal travel security (or similarly entitled) policy and associated procedures?

Answered: 210

Answer Choices	Responses	
Yes	**60.48%**	127
No	**34.29%**	72
Don't know	**5.24%**	11
Total		**210**

Q13 Which department IS responsible for the development and implementation of this policy?

Answered: 125

Answer Choices	Responses	
Human resources	**5.60%**	7
Security	**51.20%**	64
Risk management	**10.40%**	13
Legal	**0.80%**	1
Travel management	**6.40%**	8
Health, safety & environment	**5.60%**	7
Compliance & audit	**1.60%**	2
Don't know	**4.80%**	6
Other (please specify)	**13.60%**	17
Total		**125**

#	Other (please specify)	Date
1	I think it is Health and safety and HR	6/9/2014 7:51 AM
2	General	6/9/2014 7:13 AM
3	Owner	5/17/2014 5:22 AM
4	Procurement	5/15/2014 4:56 AM
5	Department of foreign affairs and international trade	5/8/2014 9:23 AM
6	All of the above	5/7/2014 11:39 AM
7	Operations	4/21/2014 1:26 AM
8	Safety and Security (One department)	4/16/2014 1:46 AM

9	more than one of the above would be responsible for developing the policy	4/15/2014 9:04 AM
10	Operations	4/15/2014 5:55 AM
11	HSES	4/15/2014 2:25 AM
12	Directors	4/15/2014 2:06 AM
13	Group Security	4/15/2014 1:50 AM
14	the departments in which staff travel as part of their main role	4/14/2014 8:14 AM
15	Insurance	4/14/2014 4:31 AM
16	Estates	4/14/2014 2:55 AM
17	Insurance	4/14/2014 1:29 AM

Q14 Which department do YOU consider most appropriate for the development and implementation of this policy?

Answered: 124

Answer Choices	Responses	
Human resources	**6.45%**	8
Security	**49.19%**	61
Risk management	**14.52%**	18
Legal	**0.00%**	0
Travel management	**8.87%**	11
Health, safety & environment	**8.87%**	11
Compliance & audit	**1.61%**	2
Don't know	**0.81%**	1
Other (please specify)	**9.68%**	12
Total		**124**

#	Other (please specify)	Date
1	Owner	5/17/2014 5:22 AM
2	All of the above	5/7/2014 11:39 AM
3	Operations	4/21/2014 1:26 AM
4	Safety and Security	4/16/2014 1:46 AM
5	Security and legal	4/15/2014 11:31 AM
6	a combination of input from more than one of the above departments	4/15/2014 9:05 AM
7	Operations	4/15/2014 5:55 AM
8	It is a collaboration between travel, security and HR	4/15/2014 3:35 AM

9	HSES	4/15/2014 2:26 AM
10	Directors	4/15/2014 2:06 AM
11	Group Security	4/15/2014 1:51 AM
12	Estates	4/14/2014 2:55 AM

Q15 Are business travel security risks a sub-component of any other policy which you have in place?

Answered: 83

Answer Choices	Responses	
Risk management policy	**19.28%**	16
Travel policy	**18.07%**	15
Security policy	**14.46%**	12
Don't know	**33.73%**	28
Other (please specify)	**21.69%**	18

#	Other (please specify)	Date
1	Travel Guidelines	6/1/2014 4:26 AM
2	Insurance stipulations	5/19/2014 3:51 AM
3	No	5/14/2014 12:31 PM
4	no	5/8/2014 9:11 AM
5	The question is a yes/no answer but the options are multiple choice. The answer is 'No'.	5/6/2014 12:48 AM
6	NO BUSINESS TRAVEL SECURITY POLICIES	5/4/2014 11:58 AM
7	No	4/18/2014 9:58 PM
8	No	4/16/2014 9:33 AM
9	no	4/16/2014 3:19 AM
10	HR	4/16/2014 2:18 AM
11	No	4/15/2014 1:28 PM
12	No	4/15/2014 12:10 PM
13	Not much elaborated at all.	4/15/2014 10:12 AM
14	No	4/15/2014 10:12 AM
15	My Clients are generally poorly equipped and educated in this matter	4/15/2014 8:58 AM
16	Health and safety policy	4/15/2014 6:00 AM
17	no	4/14/2014 3:25 AM
18	None	4/14/2014 1:20 AM

Q16 From which department IS the current risk owner (person responsible for the management of the security risks associated with business travel)?

Answered: 204

Answer Choices	Responses	
Senior management	**17.65%**	36
Human resources	**6.86%**	14
Security	**35.78%**	73
Risk management	**6.86%**	14
Legal	**0.00%**	0
Travel management	**6.37%**	13
Health, safety & environment	**5.39%**	11
Operations	**3.92%**	8
Don't know	**9.80%**	20
Other (please specify)	**7.35%**	15
Total		**204**

	Other (please specify)	Date
1	Owner	5/17/2014 5:22 AM
2	nobody as far as I know	5/14/2014 11:33 AM
3	none	5/8/2014 9:11 AM
4	Safety Management	5/7/2014 11:39 AM
5	TRAVEL IS PART OF FINANCE. NO GUIDANCE GIVEN	5/4/2014 11:58 AM
6	No responsibility assigned	4/16/2014 9:34 AM
7	there isn't one	4/16/2014 3:20 AM
8	Safety and Security	4/16/2014 1:46 AM
9	It depends. Policy, guidelines and advice pre-travel is responsibility of security dept. Once travel plans are approved, adherence to and application of security measures etc. is responsibility of the traveller and or any specialist persons required for the destination (escorts etc.)	4/15/2014 1:05 PM
10	Not addressed	4/15/2014 12:10 PM
11	Security and legal	4/15/2014 11:32 AM
12	The department that the traveller works for and the traveller	4/15/2014 3:35 AM
13	Insurance	4/14/2014 4:32 AM
14	no one	4/14/2014 3:25 AM
15	Estates	4/14/2014 2:55 AM

Q17 From which department do YOU consider the most appropriate risk owner should originate?

Answered: 202

Answer Choices	Responses	
Senior management	**18.32%**	37
Human resources	**4.95%**	10
Security	**40.59%**	82
Risk management	**13.37%**	27
Legal	**0.50%**	1
Travel management	**6.93%**	14
Health, safety & environment	**5.45%**	11
Operations	**2.48%**	5
Don't know	**2.48%**	5
Other (please specify)	**4.95%**	10
Total		**202**

#	Other (please specify)	Date
1	Owner	5/17/2014 5:23 AM
2	Safety Management	5/7/2014 11:39 AM
3	N/A	5/7/2014 7:24 AM
4	Safety and Security	4/16/2014 1:46 AM
5	depends on information the person is carrying	4/15/2014 9:07 AM
6	Falls across a number of areas	4/15/2014 3:42 AM
7	The travellers department	4/15/2014 3:36 AM
8	the traveller, organisation should provide knowledge and support	4/15/2014 2:54 AM
9	Should combine Security and Travel Management	4/15/2014 1:53 AM
10	Estates	4/14/2014 2:55 AM

Q18 In your organisation how is the travel security risk assessed?

Answered: 202

Answer Choices	Responses	
In-house	**65.84%**	133
Outsourced	**20.30%**	41
Don't know	**13.86%**	28
Total	**202**	

Q19 What sources of information are used for this assessment?

Answered: 133

Answer Choices	Responses	
Foreign & Commonwealth Office (including the Overseas Business Risk service)	**68.42%**	91
Media (including social media)	**52.63%**	70
Free online resources	**47.37%**	63
Industry networks	**57.14%**	76
Don't know	**15.04%**	20
Other (please specify)	**36.84%**	49

#	Other (please specify)	Date
1	Internal analysis teams	6/14/2014 10:40 AM
2	Australian equivalent of FCO, defence advisories	6/12/2014 12:47 AM
3	Contracted external providers	6/9/2014 11:27 PM
4	United Nations, US State Dept. Travel Advisories	5/26/2014 4:56 AM
5	also subscribe to iJET, Control Risks and other sources as well as liaison with embedded peers.	5/19/2014 9:57 AM
6	Anvil and International SOS	5/19/2014 9:19 AM
7	Personal recommendations	5/19/2014 3:52 AM
8	Intelligence analysis and risk assessments	5/15/2014 4:15 AM
9	Control Risks Group	5/15/2014 2:03 AM
10	Department of Foreign Affairs	5/14/2014 9:55 AM
11	Intelligence Sources - Armed Forces	5/14/2014 9:13 AM
12	travel security risk providers	5/12/2014 9:06 AM

13	Nothing really	5/8/2014 2:30 AM
14	CAA & EASA	5/7/2014 11:40 AM
15	In-country sources	5/7/2014 3:32 AM
16	Contextual contacts (e.g. people in-country)	5/6/2014 12:50 AM
17	Other government departments	5/4/2014 7:46 AM
18	ijet, CRF, OSAC, ASIO, Stratfor, think tanks, staff	4/24/2014 3:04 PM
19	trusted local assets	4/24/2014 2:27 PM
20	Risk advisory service	4/22/2014 10:34 AM
21	Travel risk software platform	4/21/2014 10:49 AM
22	paid for consultative resources	4/19/2014 4:29 AM
23	contracted information service providers	4/16/2014 4:35 AM
24	Security intelligence provider	4/16/2014 2:22 AM
25	Personal networking channels	4/16/2014 1:47 AM
26	Police and intelligence	4/16/2014 1:02 AM
27	Specialist foreign intelligence providers, US govt. resources	4/16/2014 12:02 AM
28	Own intel and analysis dept.	4/15/2014 10:39 PM
29	iJET, Red 24, OSAC, CRG, Our own people deployed globally, security representatives of our customers	4/15/2014 1:07 PM
30	Stratfor, OSAC	4/15/2014 12:44 PM
31	Partners	4/15/2014 12:10 PM
32	Intelligence suppliers	4/15/2014 11:21 AM
33	CIA website, Control Risks	4/15/2014 9:00 AM
34	Multi-agency approach	4/15/2014 8:07 AM
35	External Agents	4/15/2014 5:48 AM
36	other government sites, external travel security provider	4/15/2014 4:42 AM
37	CR & ISOS travel advisories	4/15/2014 4:03 AM
38	Professional travel and medical support services	4/15/2014 3:43 AM
39	Outsourced intel and alert data services	4/15/2014 3:29 AM
40	Group Situation Centre in HQ with Localized Situation centers across the globe	4/15/2014 3:10 AM
41	Government Agencies	4/15/2014 2:40 AM
42	Local source information	4/15/2014 2:39 AM
43	Outsourced service as well question 17 should have had this	4/15/2014 2:28 AM
44	Service Providers such as ISOS and Anvil plus Internal Intelligence Group	4/15/2014 2:25 AM
45	UN security briefings	4/15/2014 2:07 AM
46	In-house analysts	4/15/2014 2:05 AM
47	External specialist advisors	4/15/2014 2:01 AM
48	Insurance company support and Red 24	4/14/2014 8:16 AM
49	Professional sites provided by our insurers	4/14/2014 2:56 AM

Q20 Does travel for your organisation involve any medium or high risk locations?

Answered: 202

Answer Choices	Responses	
Yes	**73.76%**	149
No	**22.28%**	45
Don't know	**3.96%**	8
Total		**202**

Q21 Does your business provide business travellers with a pre-trip advisory or briefing?

Answered: 202

Answer Choices	Responses	
Yes	**67.82%**	137
No	**32.18%**	65
Total		**202**

Q22 Is this provided for in-house or outsourced?

Answered: 135

Answer Choices	Responses	
In-house	**75.56%**	102
Outsourced	**22.22%**	30
Don't know	**2.22%**	3
Total		**135**

Q23 Does your business provide security specific training for its business travellers?

Answered: 200

Answer Choices	Responses	
Yes	**42.00%**	84
No	**58.00%**	116
Total		**200**

Q24 Is this provided for in-house or outsourced?

Answered: 84

Answer Choices	Responses	
In-house	**76.19%**	64
Outsourced	**22.62%**	19
Don't know	**1.19%**	1
Total		**84**

Q25 Does your organisation have a dedicated 24/7/365 contact point in the event of an emergency or crisis situation?

Answered: 200

Answer Choices	Responses	
Yes	**80.00%**	160
No	**17.00%**	34
Don't know	**3.00%**	6
Total		**200**

Q26 Is this provided for in-house or outsourced?

Answered: 160

Answer Choices	Responses	
In-house	**68.75%**	110
Outsourced	**29.38%**	47
Don't know	**1.88%**	3
Total	**160**	

Q27 In the event of an incident occurring who takes ownership of the situation?

Answered: 200

Answer Choices	Responses	
Emergency/incident response team	**22.00%**	44
Crisis management team	**21.00%**	42
Security department	**18.00%**	36
Human resources department	**3.50%**	7
Health, safety & environment department	**0.50%**	1
Operations	**8.50%**	17
Don't know	**10.00%**	20
Other (please specify)	**16.50%**	33
Total	**200**	

#	Other (please specify)	Date
1	Me! Sole operator	6/8/2014 2:57 PM
2	SeniorManagement	6/4/2014 1:40 PM
3	Our regional company/regional structure	5/27/2014 10:34 AM
4	Initial response via hotline, regional guy responds and stands up the relevant people. Usually this would be the location/country manager and his team with support from any regional teams as required. Depending on the severity of the situation, country manager may wish to delegate management to any one of the depts. listed above. But the location manager "owns" the situation.	5/19/2014 10:00 AM
5	A combination of in-house security team and outsourced providers, depending on location	5/19/2014 9:20 AM
6	Me the traveller	5/17/2014 5:25 AM
7	Line manager	5/14/2014 11:40 AM

8	depends on incident type	5/14/2014 11:36 AM
9	Government department DFAIT	5/8/2014 9:25 AM
10	whichever senior management person is available	5/8/2014 8:23 AM
11	We are a small company so it'd be the directors	5/8/2014 2:31 AM
12	Probably Manager in UK. Senior manager and myself travel	5/7/2014 7:25 AM
13	Regional SVP	5/6/2014 5:45 AM
14	Senior Mgmt.	5/6/2014 12:50 AM
15	it can escalate from security dept. to Crisis Team+ Security Dept.	4/24/2014 3:06 PM
16	Myself and colleagues coordinate a suitable response	4/24/2014 2:29 PM
17	it is joint Security Risk Management	4/24/2014 4:05 AM
18	Security team, plus the crisis mgmt. team if required.	4/21/2014 10:51 AM
19	Security initially, then the BU crisis team at the asset/country	4/19/2014 4:31 AM
20	SeniorManagement	4/18/2014 8:54 AM
21	Varies according to the hours in which the emergency may arise.	4/17/2014 1:57 AM
22	Probably no-one	4/16/2014 9:35 AM
23	As yet no incidents have occurred involving overseas travel although I believe HR would take the lead	4/16/2014 2:21 AM
24	Safety and Security	4/16/2014 1:48 AM
25	Command and Coordination Center	4/16/2014 1:03 AM
26	Security or Crisis Management Team dependent on the scale of the incident	4/16/2014 12:03 AM
27	No one would know. It would be chaos.	4/15/2014 11:21 AM
28	a combination of the above departments - dependent on nature of incident	4/15/2014 9:09 AM
29	Varies client by client	4/15/2014 9:01 AM
30	Insurance Company	4/15/2014 4:59 AM
31	We have a Tier system incident-crisis	4/15/2014 2:29 AM
32	Directors	4/15/2014 2:08 AM
33	Depends on the nature of the incident. Can be Crisis management, the fire alarm team, the Health, safety & Environment department or external first responders such as the police or the fire brigade	4/14/2014 6:38 AM

Q28 From which department IS the person currently responsible for coordinating this team?

Answered: 86

Answer Choices	Responses	
Human resources	**3.49%**	3
Security	**30.23%**	26
Risk management	**18.60%**	16
Legal	**0.00%**	0
Travel management	**2.33%**	2
Health, safety & environment	**6.98%**	6
Compliance & audit	**2.33%**	2
Operations	**17.44%**	15
Don't know	**3.49%**	3
Other (please specify)	**15.12%**	13
Total		**86**

#	Other (please specify)	Date
1	it's outsourced	6/12/2014 12:48 AM
2	I believe HR and H&S at director level	6/9/2014 7:56 AM
3	Senior management	5/19/2014 3:53 AM
4	Finance	5/14/2014 9:56 AM
5	Multi-functional team headed by the GM. Other team members from Finance, HR, PR, Legal and Security	5/12/2014 9:10 AM
6	Crisis & Continuity Management	4/30/2014 12:34 AM
7	depends upon location	4/16/2014 4:36 AM
8	Country manager	4/16/2014 2:24 AM
9	The Corporate Group for Crisis and Emergency management, security and travel risk	4/15/2014 1:08 PM
10	Senior management	4/14/2014 8:17 AM
11	Faculty teams	4/14/2014 4:33 AM
12	University - Emergency Management Team	4/14/2014 3:45 AM
13	Estates	4/14/2014 2:57 AM

Q29 From which department do YOU consider the person most appropriate to coordinate this team to originate?

Answered: 86

Answer Choices	Responses	
Human resources	**5.81%**	5
Security	**37.21%**	32
Risk management	**18.60%**	16
Legal	**0.00%**	0
Travel management	**5.81%**	5
Health, safety & environment	**8.14%**	7
Compliance & audit	**1.16%**	1
Operations	**12.79%**	11
Don't know	**0.00%**	0
Other (please specify)	**10.47%**	9
Total		**86**

#	Other (please specify)	Date
1	GM, as the team cover all types of crisis/incidents, not just travel security related	5/12/2014 9:11 AM
2	C&CM	4/30/2014 12:34 AM
3	depends upon location of the crisis	4/16/2014 4:37 AM
4	Country manager	4/16/2014 2:24 AM
5	Security & Risk should be one	4/15/2014 1:20 PM
6	Corporate Group Critical incident and emergency management, security and travel risk. But them to be handed over at the most appropriate point to senior management in the respective country. It's important that Corporate take the first response then hand over to ensure corporate policy and support is triggered. After triage of situation, decision taken who to hand off to.	4/15/2014 1:10 PM
7	Business Continuity	4/15/2014 4:51 AM
8	Senior management	4/14/2014 8:18 AM
9	Estates	4/14/2014 2:57 AM

Q30 Does your organisation have a compulsory pre-trip authorisation procedure?

Answered: 199

Answer Choices	Responses	
Yes	**63.82%**	127
No	**29.15%**	58
Don't know	**7.04%**	14
Total		**199**

Q31 From which department IS the person currently responsible for pre-trip authorisation?

Answered: 126

Answer Choices	Responses	
Senior management	**39.68%**	50
Human resources	**4.76%**	6
Security	**18.25%**	23
Risk management	**3.97%**	5
Legal	**0.00%**	0
Travel management	**7.14%**	9
Health, safety & environment	**2.38%**	3
Operations	**6.35%**	8
Don't know	**2.38%**	3
Other (please specify)	**15.08%**	19
Total		**126**

#	Other (please specify)	Date
1	managers	6/3/2014 2:35 PM
2	Line management and possibly security	5/27/2014 10:35 AM
3	All travel is logged through the same system. Travel to high risk countries cannot be booked without prior approval. The system itself is maintained by Operations, however decision making on high risk travel is managed by the security team.	5/19/2014 9:22 AM
4	Owner	5/17/2014 5:26 AM
5	It's your own line manager	5/14/2014 11:37 AM

6	Relevant team/division director	5/14/2014 5:20 AM
7	Security & Head of Country	4/30/2014 12:35 AM
8	We call it security risk management	4/24/2014 4:06 AM
9	High and extreme risk locations must be authorised by Head of Security and line manager, all other locations by line manager only.	4/22/2014 3:06 AM
10	Travel Management and Security combined effort	4/19/2014 4:32 AM
11	High Risk - Security, Medium and below - Line Manager	4/16/2014 4:21 AM
12	two step authorisation combination of above	4/16/2014 1:04 AM
13	Mix of travel management, the traveller and security. Depending on the risk classification of the destination[s]. Low to medium risk destinations can be self-managed, high risk require corporate oversight as compulsory.	4/15/2014 1:12 PM
14	HoD in each DIRECTORATE.	4/15/2014 10:15 AM
15	program management	4/15/2014 8:35 AM
16	Low & medium risk the employee's manager. High risk, the security department	4/15/2014 4:05 AM
17	Security for restricted travel countries and departmental heads for cost reasons.	4/15/2014 3:30 AM
18	Dept. / Line manager	4/15/2014 12:53 AM
19	Line Managers	4/14/2014 1:43 PM

Q32 From which department do YOU consider the person most appropriate to manage pre-trip authorization should originate?

Answered: 126

Answer Choices	Responses	
Senior management	**33.33%**	42
Human resources	**4.76%**	6
Security	**20.63%**	26
Risk management	**6.35%**	8
Legal	**0.00%**	0
Travel management	**10.32%**	13
Health, safety & environment	**1.59%**	2
Operations	**7.14%**	9
Don't know	**1.59%**	2
Other (please specify)	**14.29%**	18
Total		**126**

#	Other (please specify)	Date
1	Line management and security depending on destination	5/27/2014 10:35 AM
2	Owner	5/17/2014 5:26 AM
3	Your own line manager	5/14/2014 11:37 AM
4	Relevant team/division director	5/14/2014 5:20 AM
5	Senior management and security	5/12/2014 9:11 AM
6	Security & Head of Country	4/30/2014 12:35 AM
7	Travel Management and Security combined effort	4/19/2014 4:32 AM
8	As above for Q27	4/16/2014 4:21 AM
9	Combination of responsibility. none of above adequate	4/16/2014 1:04 AM
10	As with point 30.	4/15/2014 1:12 PM
11	Fine as it is.	4/15/2014 10:15 AM
12	Senior mgmt. with input from security	4/15/2014 5:29 AM
13	As above - I set the policy!!	4/15/2014 4:05 AM
14	Combination	4/15/2014 3:46 AM
15	See 28	4/15/2014 3:30 AM
16	Combination of HSE, Security and travel	4/15/2014 1:55 AM
17	Dept. / Line manager	4/15/2014 12:53 AM
18	Line Managers	4/14/2014 1:43 PM

Q33 Are business travellers actively tracked during travel?

Answered: 198

Answer Choices	Responses	
Yes	**37.88%**	75
No	**55.05%**	109
Don't know	**7.07%**	14
Total		**198**

Q34 Is this provided for in-house or outsourced?

Answered: 75

Answer Choices	Responses	
In-house	**53.33%**	40
Outsourced	**46.67%**	35
Don't know	**0.00%**	0
Total		**75**

Q35 Which methods of traveller tracking are utilized?

Answered: 75

Answer Choices	Responses	
Reservation monitoring (ie. what is booked)	**56.00%**	42
Ticketing transactions monitoring (ie. what is actually executed)	**56.00%**	42
Technological monitoring (eg. mobile technology)	**44.00%**	33
Don't know	**4.00%**	3
Other (please specify)	**18.67%**	14

#	Other (please specify)	Date
1	iJET. Itineraries are tracked. Regional managers (like me) opt to receive alerts to the higher risk locations.	5/19/2014 10:01 AM
2	We use the Anvil system which links to our travel booking service. This allows us to see a comprehensive picture of all travellers in any location globally.	5/19/2014 9:23 AM
3	Telephone calls / emails	5/6/2014 12:51 AM
4	Anyone to high / extreme gets active tracking the rest via ticketing	4/24/2014 4:07 AM
5	Daily check-in	4/16/2014 2:26 AM
6	We use iJET. Itineraries are automatically loaded by the travel agent and Corporate Group has access to site to track, communicate with and send mass communications etc.	4/15/2014 1:13 PM
7	Track 24 gps	4/15/2014 11:38 AM
8	a combination of the above	4/15/2014 9:10 AM
9	The travel risk	4/15/2014 4:52 AM
10	Reservation monitoring unless high risk country and then GPS	4/15/2014 3:31 AM
11	Timed contact call back	4/15/2014 2:42 AM
12	Time based check in	4/15/2014 2:10 AM

13	checking in procedures, regular contact with HQ	4/15/2014 2:07 AM
14	red 24 travel tracker	4/15/2014 12:53 AM

Q36 Are business travellers supplied with important or updated security information during travel?

Answered: 198

Answer Choices	Responses	
Yes	**57.58%**	114
No	**34.85%**	69
Don't know	**7.58%**	15
Total		**198**

Q37 Is this provided for in-house or outsourced?

Answered: 114

Answer Choices	Responses	
In-house	**64.04%**	73
Outsourced	**35.09%**	40
Don't know	**0.88%**	1
Total		**114**

Q38 How is important security information provided to business travellers during travel?

Answered: 114

Answer Choices	Responses	
Email	**83.33%**	95
Text	**57.89%**	66
Intranet/website	**26.32%**	30
Mobile application	**37.72%**	43
Other (please specify)	**19.30%**	22

#	Other (please specify)	Date
1	Telephone	6/9/2014 7:58 AM
2	Combination of the above. Bulk text, email, voice etc.	5/19/2014 10:02 AM

3	The Anvil service can be set to user preference - email, text, call etc. It is also available online.	5/19/2014 9:24 AM
4	Siprnet scramble frequencies	5/15/2014 4:17 AM
5	mix of the above	5/14/2014 11:38 AM
6	Telephone calls	5/6/2014 12:51 AM
7	In the event it is a live incident we will call	4/24/2014 4:08 AM
8	Skype	4/18/2014 8:55 AM
9	Telephone Call in an emergency	4/16/2014 4:25 AM
10	verbal brief	4/16/2014 2:27 AM
11	voice over normal mobile networks, satellite phones etc. etc.	4/16/2014 1:04 AM
12	Mass communications, procedures in place for locations to call travellers. Recent example, Tsunami Pacific Coast we used a combination of all. Predominantly iJET to confirm we had a number of foreign travellers in the location. Via iJET we reach out to all travellers by email and SMS with a tick box that they mark as being ok, or requiring assistance.	4/15/2014 1:15 PM
13	VOIP / Voice conversation	4/15/2014 11:08 AM
14	combination of the above	4/15/2014 9:10 AM
15	All of the above	4/15/2014 8:09 AM
16	Phone call	4/15/2014 3:38 AM
17	via Travel Agent and Company resources	4/15/2014 3:12 AM
18	Stopped at point of departure if security situation has deteriorated	4/15/2014 2:43 AM
19	Local staff	4/15/2014 2:42 AM
20	Call	4/15/2014 2:30 AM
21	Direct call to mobile/hotel	4/15/2014 2:29 AM
22	In-house analysts	4/15/2014 2:07 AM

Q39 If your organisation outsources an aspect of travel risk management, which type of service provider is used?

Answered: 197

Answer Choices	Responses	
Not applicable	**46.19%**	91
Travel management company	**17.77%**	35
Specialist security/risk management/intelligence company	**35.03%**	69
Technological service provider	**4.06%**	8
Other (please specify)	**3.05%**	6

#	Other (please specify)	Date
1	Don't know	5/14/2014 5:22 AM
2	Aero medevac	4/15/2014 10:42 PM
3	Not Applicable	4/15/2014 10:00 PM
4	International medical insurer....	4/15/2014 10:17 AM
5	Insurance Company who in turn outsource to specialist company	4/15/2014 5:00 AM
6	Multiple	4/15/2014 3:47 AM

Q40 Does your organisation carry out any of the following procedures?

Answered: 197

	Yes	No	Don't know	Total
Pre-and post-travel security training testing	**27.41%** 54	**64.47%** 127	**8.12%** 16	197
Post trip debriefing/surveying of personnel in relation to training, planning, procedural and countermeasure effectiveness	**28.93%** 57	**61.93%** 122	**9.14%** 18	197
Interviews/observations to evaluate traveller behavior in relation to risk culture improvement	**18.78%** 37	**72.08%** 142	**9.14%** 18	197
Analysis of key performance indicators such as return on investment, incidents, morale, wellbeing, growth, staff retention, reputation and accreditation.	**27.41%** 54	**63.45%** 125	**9.14%** 18	197

Q41 Please rank the following legislation in terms of its importance to business travel security risk management (where 1 is the most important)?

Answered: 195

	1	2	3	4	Total	Average Ranking
Data Protection Act 1998	**10.26%** 20	**8.72%** 17	**24.10%** 47	**56.92%** 111	195	1.72
Corporate Manslaughter & Corporate Homicide Act 2007	**32.31%** 63	**33.33%** 65	**15.90%** 31	**18.46%** 36	195	2.79
Employers Liability (Compulsory Insurance) Act 1969	**16.92%** 33	**28.21%** 55	**43.59%** 85	**11.28%** 22	195	2.51
Health & Safety at Work Act 1974	**40.51%** 79	**29.74%** 58	**16.41%** 32	**13.33%** 26	195	2.97

Q42 Are you aware the failures linked to the management of risks resulting in the death of personnel can lead to prosecution under the Corporate Manslaughter and Corporate Homicide Act 2007?

Answered: 195

Answer Choices	Responses	
Yes	**75.38%**	147
No	**24.62%**	48
Total		**195**

Q43 Using a rating scale how effective would you rate your organisation is in relation to the management of security risks associated with business travel (where 1 is very poor and 10 is highly effective)?

Answered: 195

1	2	3	4	5	6	7	8	9	10	Total	Average Rating
6.15% 12	**5.64%** 11	**7.69%** 15	**9.23%** 18	**11.28%** 22	**6.67%** 13	**15.90%** 31	**18.97%** 37	**12.31%** 24	**6.15%** 12	195	6.09

Appendix 3.

Formal Request for Assistance

Dear ********

I am working on a dissertation in order to achieve a master's degree in security management. The topic: business travel security risk management. The title: business travel is a fact of life for many organisations. How are the associated security risks identified, promulgated to staff and effective countermeasures assessed?

A literature review has exposed significant disparity in the ways in, and extent to, which organisations are managing this function (strategically and operationally). The importance of this research lies in the fact that in our modern world business travel has become commonplace, exposing businesses and their executives/personnel to significant risk. Not only can failures in managing these risks be disastrous for the traveller but also for the business.

As part of my research I have designed a short multiple choice questionnaire (under 10 minutes) for business leaders and security professionals which will enable me to examine current practice in order to create a comprehensive overview of the topic. The questionnaire does not request any personal information from the respondent, and no personally identifiable information is obtained through completion of the questionnaire.

Please can you use the link below and complete my questionnaire (hosted by SurveyMonkey).

I would really appreciate your assistance.

https://www.surveymonkey.com/s/BusinessTravelSecurityRiskManagement

Yours sincerely

Gian-Rico Luzzi

Tel: ********

Email: ********

Appendix 4.

Supplementary Request for Assistance

Dear ********

I am a Loughborough University post graduate student working on a dissertation in order to achieve a master's degree in security management. Mr Danie Adendorff is my supervisor. The topic: business travel security risk management. The title: business travel is a fact of life for many organisations. How are the associated security risks identified, promulgated to staff and effective countermeasures assessed?

A literature review has exposed significant disparity in the ways in, and extent to, which organisations are managing this function (strategically and operationally). The importance of this research lies in the fact that in our modern world business travel has become commonplace, exposing businesses and their executives/personnel to significant risk. Not only can failures in managing these risks be disastrous for the traveller but also for the business.

As part of my research I have designed a short multiple choice questionnaire (under 10 minutes) for business leaders, security and human resources professionals which will enable me to examine current practice in order to create a comprehensive overview of the topic. The questionnaire does not request any personal information from the respondent, and no personally identifiable information is obtained through completion of the questionnaire.

I would like to distribute the questionnaire as widely as possible within the selected sample group (preferably via email or moderated LinkedIn group). I have been successful in gaining access to security professionals through The Security Institute, and business leaders through The Institute of Leadership and Management. However in order to ensure the validity of data obtained in my research i need to have a significant response level from human resources professionals.

This is due to the fact that a Global Study (link below) conducted by Professor Lisbeth Claus (a prominent US Human Resources Expert) has highlighted that human resources is predominantly responsible for the management of business travel risk.

Claus, L. (2011). Duty of Care and Travel Risk Management Global Benchmarking Study, [Online]. Available at: http://www.internationalsosfoundation.org/resources/white-papers/

I have had a fantastic response to the questionnaire thus far and I expect this questionnaire will be of considerable interest to your members as this subject is quite topical. Can you please assist me or put me in touch with someone who deals with research access requests.

Your assistance would be much appreciated.

Yours sincerely

Gian-Rico Luzzi

Tel: ********

Email: ********

Appendix 5.

Questionnaire introduction

Thank you very much for agreeing to take part in this questionnaire, which should not take longer than 10 minutes to complete. This questionnaire is part of a research project to examine contemporary business travel security risk management in the United Kingdom. Your responses are important in enabling me to obtain information regarding current practice, in order to form an overview of business travel security risk

management. Please note that all data provided will be treated in the strictest confidence to ensure anonymity. You will see that your personal information is NOT requested at any stage of the questionnaire. There will be space at the end of the questionnaire to leave your personal details for the sole purpose of allowing me to share the results of my research with you, if you wish (subject to permission from the Programme Director at Loughborough University).

By clicking "Next" you are confirming that you have read and understand the information about the project above, understand participation is voluntary and agree to the anonymised use of data in my dissertation.

Source: own work, Luzzi (2014)

Appendix 6.

Interview Request

Dear ********

Thank you very much for taking the time to complete my questionnaire. I have been well supported by The Security Institute, ASIS UK Chapter 208, the Institute of Leadership and Management, the HR Society, the International Professional Security Association, the Association of University Chief Security Officers, and have had over two hundred completed responses thus far.

The next phase of my research involves the compilation and analysis of qualitative data in relation to business travel security risk management. My objective is to conduct interviews with the people responsible for the function within a small number of organisations, who have travelling personnel and executives, in order to interpret and validate the questionnaire results.

The interview questions would be similar to those asked in the questionnaire, however the interview will allow me to get richer data and 'add some colour' to the grey areas. The interviews can be done on a completely anonymous basis if preferred. If however the interviewee is happy to be recognised then I would be more than happy to acknowledge the assistance in my dissertation.

If you are the person within your organisation who is responsible for the function would you be able to assist me by affording me the opportunity to interview you (or your colleague who is responsible for the function). I am happy to travel to your workplace or any other location convenient for you. I expect the interview should not take more than 30 minutes.

I do understand that the research encroaches on to a subject which is really topical and involves sensitive data, but I can assure you that I would take every precaution to ensure you and your organisations anonymity and confidentiality if required. If you would like to verify my particulars please feel free to contact my programme director at Loughborough University, Mr Danie Adendorff.

Your valuable input would be greatly appreciated. However please do not feel obliged to accept this request.

Yours sincerely

Gian-Rico Luzzi

Tel: ********

Email: ********

Appendix 7.

Interview Template

Interviews 03/06/2014

I am a post graduate student currently studying at Loughborough University. I am currently working on a dissertation in order to achieve master's degree in security management.

The project that I am working on is looking at how contemporary organisations manage the security risk associated with business travel.

The aim of this interview, which is one of three, is to examine the current state of the practice in the United Kingdom and the ways in which it is carried out.

I would like to use the data obtained from this interview in my dissertation and to correctly reference you. However I am also happy to keep you and your organisation's identity completely anonymous if you prefer.

To save me from having to try and write down and remember everything discussed today would you mind if I electronically recorded the interview using a voice recorder. This is saved securely and is purely to help me transcribe the discussion. This can be switched off at any stage if required.

Do you have any questions or comments?

1. When considering the strategic aspects of managing business travel security, in your organisation and/or experience who are the key stakeholders involved?

   Senior management / security / risk management / legal / travel management / health & safety / operations

- Who is the risk owner (overall responsibility)?
- Is the traveller seen as a stakeholder (shared responsibility)?

- Would you say there are stakeholders more suited to the role?

2. When considering the operational aspects of managing this risk, in your organisation and/or experience, how are the business travel security risks assessed?

- Identified and analysed in-house or outsourced?
- If in-house - by who, using what methods/sources? Is it a continuous function?
- If outsourced – what type of service provider (consultant or specialised travel security provider)? Is this on a continuous basis or only when required?

3. In your organisation and/or experience how are identified security risks promulgated to personnel?

- Policy (specific or part of another)
- Procedures (compulsory pre-trip authorisation)
- Training (pre-trip advisory; security awareness & specialised security training)

4. In your organisation and/or experience what other countermeasures are used to manage this risk.

- Transfer

  Insurance including specialised kidnap & ransom insurance

- Avoidance

  Refusal to travel

  Limit/restrict passenger no's

- Reduction

  Emergency contact (in-house/outsourced?)

  Security updates via email/text/phone/website/app

Specialist services: flight and expense monitoring, security & medical services, technological including tracking

Emergency/crisis response teams

5. In your organisation and/or experience is the effectiveness of the travel risk programme evaluated?

- By pre/post trip testing to see if the training was effective
- By debriefing/surveying personnel to evaluate training, planning, procedural and countermeasure effectiveness
- By interviewing/observing to evaluate traveller behaviour in relation to risk culture improvement
- By analysing key performance indicators

Return on investment (lower insurance costs)

Better morale

Incident level reduction

Increased productivity & well-being

Increased staff retention

Accreditation

6. Have you ever encountered a serious security incident involving business travellers and if so how was this managed?

7. Free comments.

Appendix 8.

Transcription Interview One

Interview 1
03/06/14
11:13

RL: So before we start do you have any questions or comments?

P1: No none at all.

RL: Ok. So when considering the strategic aspects of managing business travel security in your organisation or in your experience in general who would you say the key stakeholders that are involved?

P1: Corporate security and HR tend to manage what programme we have, the other stakeholders clearly are the individuals themselves and we work in fairly siloed divisions so you end up with people not talking to other people so somebody at the top level corporate structure has to pull it together and that one person that one individual is me so I'm the major stakeholder in ensuring that the program is there and monitored and run effectively and that's from corporate security. The rest of the time it's probably I mean other stakeholders would be our main travel agents or MTA's, our executives, our stakeholders because they own responsibility, due care and diligences to their employees, but there is a general laissez-faire at the top level in our company that the risks are just not going to happen, so they may be there but they are manageable and currently there is no great drive from the top to push any kind of strategy forward.

RL: Would you say you are the risk owner?

P1: I don't own any risk and this is something that corporate security never does. The risk owner is with the line managers, so if you are sending an employee away we provide the line manager with the tools to make that assessment. We do not, and we

stress on a number of occasions, we do not own the risk at all we are just risk advisers and how to deal with the risk and mitigate it.

RL: OK. In your organisation would you say that the traveller is seen as a significant stakeholder? Would you say that, in my questionnaire there is a sliding scale so would it be seen as an equal fifty-fifty share of responsibility?

P1: I am going to refer back to my research as well which I am absolutely happy to provide you with a copy and I asked that question in my research and mine was predominately from within my company employees so I know that most of them feel that it is a fifty-fifty share that the company has a duty of care and you are well aware of all the legal duty of care implications, corporate manslaughter act etc., but the individuals also all agree that they have a duty of loyalty to the company to make sure that they had prepared, had got the information they wanted and I was very impressed in how they had prepared for that so I delved a bit deeper into that, so I would absolutely agree that it is definitely a split and I would say that the split is either fifty-fifty or sixty-forty in favour of the company. The company does more but the individual should actually bring it up to fifty-fifty in reality.

RL: The departments that you have within your organisation.

P1: Yes

RL: Do you literally have all of them, HR, Legal, travel?

P1: We have no travel management so where in an ideal world you would have a travel manager, we don't have that in our company. We are a FTSE 100 company, 12/13 thousand people now working out of 41 countries but we don't actually have a travel manager so it is left down to individual line management or divisional managers, divisional executives to make their own decisions based on a set of guidelines which is fairly nebulous. But apart from that we have every other function.

RL: Yes. Would you say that there are any other stakeholders who would be more suitable to the role than yourself as a manager?

P1: I think if you had a travel risk manager or a travel manager as many other larger companies have that look at the, not only the risk but also for example look at the economy scale, hotel choices, travel choices looking at the economic side of that as well as looking at the security I think that would be ideal but we don't have that so do I think there should be, yes I do, do we have something like that, no we don't, is there anybody currently better suited to do it than corporate security, probably not. Simply because nobody is looking at the travel management as a whole structure they are looking at little individual bits of that travel management, risks, travel risks, economies are looked at within divisions so one division will team up with British Airways, one will team up with Virgin there is no cohesive structure to achieving economy of scale if you like.

RL: Now moving onto the operational aspects of managing the risks in your organisation and experience how are your business travel security risks assessed?

P1: We use a third party company called Ijet whom I'm sure you are aware of. I have used them for about 7 years now. We progressed from just a database, hooking into their travel database to provide intelligence, to actually now traveller tracking so on domestic journeys we just note the travel and the traveller gets very little additional information but it is on a database. On international borders including North America, so Canada, US we actually get that information but it is actually pushed to the traveller or alerts and warnings and risk mitigation. On top of that I as the owner of the system, not the owner of the risk but the owner of the system, or sponsor of the system, get notifications if people are travelling into high risk countries designated by Ijet as high risk so they do it on a 5 curve 1 sliding scale so anything over a 4 or 5 I get notification of but our system in the company doesn't, apart from 1 small business. So from the Ijet point of view I look after the system I will be notified, but as I said, one small business does pre-travel advice, in-effect goes through a questionnaire, none of the other businesses do. So the vast majority of people will get no other pre-travel advice apart from that which is pushed by Ijet itself which is a failing on our part. We need those that are going to these high risk countries and have a system in place that makes the line managers assess the risk of their employees and it is something that we are getting to but are not there yet.

RL: So, like a compulsory notification?

P1: Yes. The problem that I have is that the travel data collection through Ijet is not compulsory in our company, it is not mandatory.

RL: OK.

P1: So if you happen to use a travel agent that is linked into Ijet all well and good, if you don't or if for example you go on the web and book a low cost airline it is down to the individual who is encouraged to manually enter that data. Now if you are looking at a travel planner or PA, most of the PA's around the bazaars are ok, they try and do it, but if you are looking at individuals, middle managers who don't have that admin support they won't do it, and so I will never know if they have gone into a high risk country even on a low cost airline so I think even now Easyjet flies into Moscow so you will have that issue in Moscow and you will never know if someone has been in and out of there. So that there again is a big failing on our part is that we don't grab all of the data of every single traveller. So, for example, when MH370 went missing, and is still missing, I did my checks on Ijet and all I could say to the executive was to the best of my knowledge and belief we have no travellers on there, however I don't know and so that undermined the whole of the Ijet system because the executives say well you can't tell me 100% and my argument or my counter argument well you won't make it mandatory so how can I tell you if you don't make it mandatory. So we end up with that kind of impasse, nobody's grasping the nettle at the highest level to move that on. Did I answer your question?

RL: Yes. So in your organisation once again, we are looking at, how are the identified security risks promulgated to personnel?

P1: I would probably use a case study for that, it is easier, how I looked at, what I have done recently, we did the Ukraine and recently Thailand. Clearly the media strikes and everybody knows about the Ukraine and then Ijet escalates. Thailand is the same, we looked at it and saw it escalating. We looked at the Ijet, we take the FCO advice as well, that's actually self-driven by us in corporate security, in fact self-driven by me, I lead on it, if not one of the other 2 operatives will pick it up, but usually it is me. You then

have to make that assessment and that call as to you advise people against travel and our company tends not to do that, and very similar to your original question, is that I get it from the managers, is well what is your advice you own the risk, in corporate security, no we don't Mr line manager you own the risk, you can send people but all we are asking that you do is you make that assessment you look at what your risks are to your employees you give them every possible opportunity to mitigate those risks and then you do the normal risk mitigation you either transfer the risk, you avoid the risk, all the good things. In the case of Thailand I had four people going out last week and the executive director made the decision based on one of his general managers advice to let them go, and he based that, he came in a saw me and said look we hear what you are saying about we advise you against but it is only an advice, however we decided that in this case they had BGs so they were being met by Thai officials, total bodyguard throughout, and it was in a non-issue place really a non hectic place so we said fine, you have done everything we asked, you have done the risk mitigation if it all goes wrong then it is down to you. So what we tend to do we observe, we watch politics around the world, any hotspots. We don't operate a great deal in the Middle East but we have a small business of about 600 people that actually do pipelines, oil pipelines, so they are into the Nigears, place like that in Algeria, where we will actually have those people so we have to look out for any hotspots. We then take the initiative and we will put out appropriate advice, that said Ijet have also taken the initiative and that is why we pay them is to send out warning critical information emails to the travellers in advance to say there is a legionnaires disease broken out on this plane if you are travelling out on that which we know you were you might what to get checked out, or this has happened in Thailand avoid this area so again it comes back to that the traveller has to take some responsibility for their own safety and travel plans, and ultimately the traveller should be able to, without any kind of recourse, say actually I am not happy with my own personal safety and therefore I don't want to go on that trip. We try and encourage that in the line managers and I think we are kind of getting that through. So that is how we tend to deal with it, it is very reactive I have to say but then most things are in the World. We can be as proactive as we can by providing them with intelligence but I am not to know if there is going to be another ash cloud tomorrow in Reykjavik or there is going to be a mass demonstration in Hong Kong, I don't know we can only go on the intel that is out there through a third party at the moment.

RL: And about policy now – your policy which relates to this risk is it a dedicated policy?

P1: I can tell you in one word what our policy is, fragmented. We have a very high level policy of, as I mentioned, you are encouraged to use Ijet, if you don't use one of the main travel agents, the MTAs, that are linked into Ijet then we encourage you to put the data on, or you should put the data on manually onto Ijet, it doesn't happen, a lot of the time it just doesn't happen on the manual entries. Automatic entries no problem and the people know which ones those are so that the top level is very cuddly it is very friendly approach, we are not a big ogre that puts out black and white which is in some cases unfortunate. So we have a top level strategy of advising people what our policy is per say as it is. What to do in the event of an emergency, where to go, how to do that, and behind the scenes the policy for me is that I have protocols with both Ijet and any of my security command centres 24/7 that Ijet will phone into so we do that, but as far as the user is concerned it is fairly transparent and it is fairly hands offish by the big bad ogre of corporate. So there is no definitive travel policy. If you said to me what is our travel policy in the book? There isn't one, and if there is it will be in a division only. It won't be across all the businesses. So unfortunately fragmented.

RL: We touched on already procedures looking at compulsory pre-trip authorisation already. Looking at the training that is going into the personnel to highlight the risks and the ways in which they are supposed to look after themselves, look after company information, company assets. The pre-trip advisory you spoke about through Ijet already. Looking at security awareness training do you have any formal training, are all the company employees specially trained?

P1: No, we employ a third party company called The Security Company to provide, in fact we introduced it last year to provide a full educational programme including a website, which we host internally, including videos, educational videos and campaigns. We introduced this in October so we are about half way through the first year of doing this. I think it is just difficult to quantify just how much has been taken in so we are looking at a campaign to try and assess just how effective the campaigns have been. Travel isn't a core area that we have looked at in that training at the moment. I have asked for it to be in there and it will probably be in the second tranche so we will be

looking at here's how to keep yourself safe when you travel, some travel tips, probably some websites but at the moment I tend to be pushing things out as and when I see them on our homepage so a bit ad-hoc really but there is a formal programme it just doesn't include at the moment a full assessment of travel risks, it will do though. As I say there is only 4 of us now and I am down Shanghai next week to interview a 5th one but there is only 4 of us on the team to cover global. So resource wise we have to outsource.

RL: When it comes to really high risk locations would you go so far as to organise HEAT or CONDO training, that level of training for employees?

P1: We have not done. I have been in the company 12 years and we have never had probably risk assessed as that high. The executives don't think that they are that high profile enough for K & R, again that is probably a misconception but nevertheless, they don't think they are. We don't travel to places that are somewhat regarded as the hot spots in the World, having said that we have a site in Mexico so clearly people are travelling to and from Mexico City and some of the other areas in the world where, if we knew that they were going into one of those 4 or 5 areas I would then assess with my boss to say actually they need some help they need a bit more than just going in on a wing and a prayer, they need to have EP and when I have spoken to our Executives they are vaguely aware that they would need it if they went into those places but they don't believe they are going to those places where historically K&R actually occur, clearly that can be on the streets of London but they don't think like that so, no we don't it would be picked up on that 4/5 and I would know somebody is going in there the problem that I have is that my Chief Exec's PA books his travel through a private company that doesn't link into Ijet and his PA still refuses to put his travel onto Ijet so I have no clue where my CEO is. So that's the type of thing that I get, you know it is kind of frustrating, it's fragmented, it needs a cohesive approach and for a FTSE 100 company it is slightly surprising.

RL: Looking at the counter measures that are used, obviously we have got the transfer, the avoidance, the reduction, apart from the ones you have already discussed would you highlight any other methods that you are using?

P1: Yes, we would use third party specialist agencies for things like EP work or route surveys. Ijet also provide a very good service as do CRG we have some links with CRG on an assessment or Intel of a particular location if it is outside the norm. So a particular hotel in Mumbai they may be able to give us information on it, if it is outside the norm. I mean the Oberoi and Taj Mahal are normal ones now, but other areas like Navi Mumbai, if we start using a particular area in Navi Mumbai we may kick it to them and say what do you know about this location any intel on it. So we will use that third party but apart from that nothing else.

RL: Do you limit and restrict the passenger numbers of people flying together?

P1: Yes, we try.

RL: I suppose it is very difficult when you don't know where someone is flying?

P1: It is hugely difficult, because a) you don't know if some of them are flying or not b) you have this siloed division so a divisional director may say I only want four of my guys in the whole division to travel on the same plane. But another division has another four guys, so we at corporate level, at the high level go hey guys, hold on you can't do this and they come back and say well actually we can afford to lose four guys and the other division can afford to lose four guys, and this is how they think, but so in theory actually thank you very much but we're ok. So that is their risk assessment and I have that almost on a daily basis I have that argument, and I get my Ijet notifications I look at anything rated over four, I don't actually do anything with fours but I do with five and definitely six, seven, eight, nine and tens. We had our company conference recently and I had exactly that argument, people saying, and this is the top one hundred people in the company, all flying to Singapore. Usually Singapore is fairly restrictive airspace so you have these optimum BA flights that they were travelling on and I had that that answer back, that we had maybe ten people on the flight but only three of them were specialist in this area three of them are specialist in that area. Devastation to the company as I believe it was with MH370 and I can't remember I might be misquoting but I thought it was IBM, one of the big companies had a number of people on there and it doesn't matter whether they are good at a particular role, the devastation across the company is huge. Yes we do, is it well enforced, no it is not. As well as things like

will we be recommending I am writing a paper based on my research to recommend certain changes in the system – one of that will be tell me what you want Mr CEO we are having a change of CEO's – tell me what you want and then we will implement that but he has come back to us and said well tell me what you think I want which is all very difficult if you don't get that assistance.

RL: Emergency contact, you've said that's through Ijet?

P1: It is through Ijet predominantly, if indeed they are registered on the Ijet system and they have that trip registered. They are provided with a welcome email when it's first registered. It's hey I understand you are going to Johannesburg on this flight, here's a trip review if you want to read it, it's up to you please ensure that you register and that all your contact details are there, here's all the emergency numbers that you need. Then we have a 24/7 emergency number out of the US North East, which as I say there is a system behind that which provides them with a list of protocols. So we have covered medical emergencies, Medivac, terrorism, through to lost passports, through to lost tickets and how each of those levels are dealt with. The more serious issues are put through to the company in one of our either Canada or the UK, UK primary, Canada secondary, and I might introduce a tertiary into Asia but there is always a language barrier with Asia so I can't do sunrise/sunset but I can cover most of following the sun through on a response active company level. So when the person phones up this fairly anonymous, although it is a company branded telephone line they will get probably pushed through to our company to somebody that can do something about it within about 7-10 minutes. So that is kind of my aim I don't have any KPI's but my aim is within 10 minutes of somebody phoning up saying help, that we actually get them through to our company and then we, as a security operation, are pushing it through to the HR Directors, which is what we have agreed with them that they will be cascaded through within their division. So within 10 minutes there should be somebody saying I know who you are, I know where you work, I am prepared to help.

RL: Then HR take the lead from there?

P1: HR will take the lead, we have provided that assistance unless it is something like K&R which has a huge security influence, or terrorism we may be called into a crisis

management committee but apart from that HR will take the lead with that Medivac, lost passport that sort of thing.

RL: And something highly security oriented?

P1: We would be part of a crisis management team.

RL: Obviously Ijet do everything, its flights and its monitoring?

P1: It doesn't do expense.

RL: No not expense.

P1: No we have just taken on Concur, so we are going to look at expense monitoring. I have no clue, one of the issues I have is that I have no clue on how much is spent on travel which goes back to my point of who would be a key stakeholder and that would be a travel manager who would be able to grasp that from across all of our divisions. Currently nobody has any idea on how much we spend. You could micro it down to the divisional levels but even then it is difficult so even if we try to get that information we can't, so they don't do travel expense, nor do they do any kind of personal expenditure when you're travelling that's through, currently, individual excel spreadsheet based systems. We are just trialling, in fact I have just started this week trialling Concur so we will be doing it electronically.

RL: And the technological systems that you use. Are you actively tracking people, using technology?

P1: Tracking is that what you mean.

RL: Yes

P1: No we are not. One of our recommendations will be. Currently there are three ways you can track somebody. There is the itinerary based, which is a non-live based scenario where you are hoping that the person who says they are going to be in Shanghai didn't

go to Beijing or somewhere where the bomb has gone off, and if they go off-piste you have no clue where they have gone. To the other extreme where you have GPS tracking, which is usually through a mobile device of some kind, smart phone. But that would require full consent. It also breaches a number of laws, certainly European Laws, such as French, Belgian and Holland. Privacy laws are very strict there on what you can and what you can't ask your employees to do, so there are huge legal implications of doing that, of mandating it. A voluntary one you could possibly do that with a compromising GPS. The other way is using a push technology from the employees. So an app on a smart phone or a tablet where they check in, and it is down to them, again due to loyalty, to take the initiative to go ok here is my app this is what I want and we can check in. We have looked at the Ijet one, we are currently also looking at another one, it is basically push technology. You will physically have to turn the GPS on if you want to be tracked you have to push the button, there is an emergency button for all hell breaking loose and I think most of them are very similar. CRG have one, Anvil have it, all the major players.

RL: Once again we are looking at the travel risk programme, how is the effectiveness of this programme in your organisational experience actually evaluated. I know you mentioned just now that you are looking into evaluating your training?

P1: I will be quite honest with you Rico I don't think it is evaluated. I mean the effectiveness of it is not evaluated. I guess the effectiveness of it is when something goes wrong, that's the evaluation. Did it work or did it not work. We have done some test scenarios with Ijet to see if we can make the whole protocol and system work, but actually return on investment and evaluation of effectiveness, it's not done.

RL: Would you say that that's a cost implication?

P1: No it is a mind-set implication. I think to make it effective you have to prove that there is cost involved and that there's a grabbing back of costs in some ways. I think you have to prove that the return of investment is there and you have to get the mind-set of the people that have to do that as well, and as I said right at the beginning when you don't necessarily have the cohesive support, and I am not saying they are unsupportive, they are just a difficult forum to get all in one direction. Our head

executives will have a lot of different opinions and then, you never end up with clear concise guidance. So actually if you don't have a proper system in place, then to evaluate the system we have is probably non-productive anyway. You need the proper cohesive system in place and then you can provide KPIs, then you can provide an evaluation of how effective that system has been. So as I said at the moment MH370 to the best of my knowledge and belief that is not a good statement to start with. I would probably still say it no matter what but if I had a more cohesive programme where I knew people were mandated to use it I would have more confidence in that statement. To the best of my knowledge and belief and I really do believe this there is nobody on there, but I couldn't say that at the moment.

RL: And one last question – Have you encountered, over the years, serious security incidents involving your business travellers, if so can you just elude to what they may have been or how you have managed it?

P1: Well one springs to mind immediately which involved me in Moscow with somebody, I was walking down the street with a colleague, just outside of Red Square, and somebody dropped a wad of dollars in front of me, and your natural reaction is to say oi, you just dropped something and as you go to pick it up to give it him back then a Policeman comes out of nowhere, alleged Policeman comes out of nowhere in civilian clothes and says you have just tried to steal this you need to come with me, show me your wallet, show me some identification in which case the warning bells come in at that stage, no wallet comes out, I am lucky enough to speak enough Russian to get by so I said no problem if you are a Policeman lets go to the Hotel and we will go to the reception and we will call your colleagues as well, at which stage, to cut a long story short, they shot off and nothing happened but that was because we were sensible enough with our training to know something is wrong here, this isn't quite right. We've had major traffic accidents, we have had somebody actually crippled in a traffic accident in Macedonia, covered with by HR and this is before Ijet really came into its own. I'm not even sure if they would have phoned Ijet anyway I think they would still have gone the local hospital route. We casevaced him back and unfortunately he has been disabled now for life, that was a drunk taxi driver. We have had nothing major, and I monitor all the calls into the emergency centre and in the 2 years that I have been running it fully, I've had ten calls into there and most of them have been about lost passports. So

you could say is that a measure of success or is that a measure of ignorance, I don't know and that's my problem I simply don't know. I could rest my laurels and say look we are doing brilliantly because nobody is having a problem out there I suspect that's not the case they are just not reporting it. Laptops stolen all the time so that tends to go through the IT route. We have had nothing major, we have had, going back 10 years, we have had kidnappings of people in Brazil where our General Manager was taken by a local gang and was basically take me to your plant and give me all the gold and the General Manager said actually I am not part of that division at all my factory deals in, what we call frits which is a sand product and glassware and they said no we don't believe you take us to them and we will, a tiger kidnapping, hold your family hostage and he took them to the factory and he went there you go there's the sand and they went bugger ok let the family go and nothing happened. He didn't even bother reporting it so 6 months later somebody found out over a beer that that had happened and he said oh that is just Brazil. So we haven't had that sort of total experience. I guess the closest we ever came, we had two people in the Oberoi, in Mumbai, the day before the attacks by Lashkar-e-Taiba, and we didn't know for another two weeks afterwards that they had been in there so I guess that really was the catalyst for getting the traveller tracking in, apart from that nobody's really taking it, I'm not saying nobody's taking it seriously, but we haven't perhaps had the understanding and support, and that maybe our issue of not getting them to understand what the risks are so I am hoping that my recent research into it and I have released my findings to the Board, but interestingly enough I gave them my dissertation 2 months ago and I had 1 of 12 people in the top directorate, so it went to 12 of them, and 1 person came to me in the corridor one day and went yea very interesting I only got to the exec sum but very interesting and that is the only feedback I had from 12 people in charge of the company on risks where you are saying to them you're fragmented and you are at risk you know from a corporate governance and a corporate compliance, corporate duty of care you are at risk and they said well we will wait and see what your recommendations are then. So you can see it's a struggle. But I have a clear picture of where I want to go, clearly when we don't have the issue of these incidents occurring all the time people say there is no threat and it only takes one major issue and the threat becomes very real. Luckily, touch wood, we don't have issues day to day we don't operate in particularly hostile environments.

RL: That sums up my questions I don't know if there is anything else, free comments.

P1: I had a wonderful quote when I did one of my interviews by a lady, senior manager, and she was chatting away during her interviews and one of the questions I asked, because I was more of a personal rather than a corporate looking quite strategically at this I was looking on a one to one personal so I went down a level and didn't worry too much about the corporate, and I said what's the biggest risk you face when you're travelling and she said the drivers, she said I get into a car, she said it could be a taxi cab or it could be a driver sent for me but I am a single female to start with I get into a car and they drive like maniacs, particularly in Asia, so we chatted on a bit and I said well how can we mitigate that for you, chat, chat, chat and she said do you know what we tend to look after our people, no we tend to look after our cars more than we do people and it was an interesting comment and it was very much a case of you are absolutely right we do, people look after their cars, they buff them, they shine them, they look after them they don't want them dented, they take avoiding action they don't go into traffic jams, you know all the things we don't actually do in our personal life when we travel. So that was an interesting quote on that looking at a very basic level about self-preservation. But apart from that it's a struggle that I've proved to them that other organisations that do have cohesive. I have looked at a number of case studies on major companies. Different ones have different ways of looking at it. Look at somebody like Google, if you haven't already, their strategy for notifying, Google is a different company anyway their whole work ethos is probably different from the structured traditional approach that we would expect and theirs is one of volunteering information on where they are going but also incentives where if you can get the hotel cheaper than their published price you get halve of the share back or it goes into a pot and goes to charity or something like that so they have got an innovative way of doing it and they seem to be able to measure the success of that. We are a more traditional type of company, I suspect we won't go down that road but it's certainly another option.

Appendix 9.

Transcription Interview Two

Interview 2
03/06/14
14:09

RL: Before we start do you have any questions or comments?

P2: No

RL: When considering the strategic aspects of managing your business travel security in your organisation or just your experience from other companies who are the key stakeholders that are involved?

P2: Ok, so this is global travel.

RL: Yes

P2: Ok, internal stakeholders are HR, legal, we have a travel management team who basically deal with everything around travel apart from the security aspect. External we've got a third party travel risk management company, so we use a company called Ijet which is linked back to American Express, that's purely an intelligence tool and data analysis really they don't have any impact on where we go or how we go there it is purely an intelligence and information source. External also Government agencies obviously from the point of view of UK travellers we may look at the FCO, if its US travellers then we may look at the State Department for travel, or any other Government Foreign Office really depending where we are off to, were we are going.

RL: Who would you say is the risk owner?

P2: That's an interesting one. I would say it is probably not defined as much as it should be. I would say it is pretty much 50/50 between the travellers themselves and the individual business unit.

RL: In the business unit who would take the lead security, risk management, HR, Legal?

P2: So just in terms of security?

RL: In terms of assessing and managing the security risk.

P2: That would come under our team so we are the global security office, so we work across the business across the globe. So there is a team of us so we've got field based in the UK, North America, Lat-Am, and we basically cover the globe in terms of security risks. But we don't really own the risk as such.

RL: If you had to name a stakeholder which would you say would be best suited to be the overall risk owner if it was clearly defined?

P2: If it was then it's a real tough one, it would probably be the senior manager in that business unit so the Managing Director for that particular business unit. Personally I don't think it should be HR, I don't think it should be legal can't be risk management. It shouldn't be us.

RL: From the literature review it seems like HR worldwide are responsible?

P2: Yes I think that HR get involved from a due diligence point of view and a duty of care and all those types of things but they tend to have little input in the security aspect, they certainly get involved but whether or not they own the risk, that's not my experience.

RL: Well the studies have shown that globally HR is leading and in Europe security is taking the lead.

P2: Yes it's interesting.

RL: There's a slight difference between Europe and the rest of the World.

P2: Yes, Yes.

RL: Now moving on to the operational aspects of managing this risk in this organisation or your experience, how are the business travel security risks assessed?

P2: We obviously use our own data that we have got globally, we have offices based in 46 countries, so we can get that in Country information as well. Most of it comes in from a security perspective from external stakeholders, Ijet we would use, as I say Government foreign offices, media, social media all those. It's one big pool of data and see what comes out of the middle of them then really. So I think Ijet is our main tool in how we factor whether we travel to a region or not so they score from one to five, one's lowest five's highest so if it's a five we are talking places like Iran, Afghanistan which we haven't got business in but they are no goes for us. Four is a high risk so something like Bangkok or Thailand who recently went up to a 4 because of all the civil unrest or Ukraine or something like that. So that's what we gauge our travel on because it's consistent globally and it delivers the same message, it's based on the same criteria. We can override it, we can upgrade it or downgrade it if we think there is less risk or more risk but that's pretty much what we use as a business.

RL: So it's a combination of internal and outsourcing?

P2: Yes

RL: Is it a continual process?

P2: Yes

RL: Are there people that are constantly monitoring worldwide events in house that are constantly looking at situations or is it done per trip?

P2: No it's not per trip. So when someone books a trip they would automatically get a trip brief via the system. If that's a Country of a 1, 2 or 3 then we are not notified of that trip so if someone's travelling to the UK or France or Germany, somewhere like that that's just a normal go about your business as normal just with the basic security precautions. If it's a 4 then we will be involved as a team and we may provide some additional security advice or guidance. If it's a 4 or a 5 then potentially we may supply additional security in Country so there may be some EP work, meet and greet, ground support or whatever. It really depends on where it is. We don't have a travel security team specifically it comes under each separate regional security manager to provide that guidance falling back on those sources that I mentioned.

RL: Yes, ok. Next question relates to how are these identified risks promulgated to your personnel, the methods whereby you make them widely known?

P2: We have an intranet site, internal site that we can put information onto. If it's a particular issue, say with Thailand recently for which the risk did increase for us so we put out internal bulletins just to let all staff know that there was an increased risk. If we've got staff in Country in an office then we would reach out to them direct just check everything is ok, they are safe and secure and if there is anything we can help with. We don't really do a blanket update for staff on current risks across the Globe, Country by Country it's more of a case by case basis. Maybe it should be more proactive but it tends to be quite reactive.

RL: Do you have a dedicated policy, a travel security policy?

P2: No

RL: Is it part of another policy?

P2: So in part it comes under the global security policy, in part it comes under the global travel policy but we don't have that policy in the middle which is a dedicated travel security policy. It is currently being written at the moment. I have bought a copy of it with me actually. It is something that we are working through at the moment writing a

dedicated policy just for travel security. But one of the issues goes back to your previous question around who owns that policy, so that is an interesting one.

RL: OK. Looking at some of the procedures that are used to promulgate do you have a compulsory pre trip authorisation?

P2: Only on certain criteria. So if it is a high risk country or if it is a country where we blocked travel. If there is more sort of general travel policy, so if someone booked a flight but didn't book a hotel, then there would be a pre-trip audit by our travel team, but in terms of security those are pretty much the main pre audit things. High risk and blocked Countries.

RL: Are personnel forced to book their travel through your travel management company which then goes through Ijet?

P2: Yes. So we book all travel through Amex. That feeds into Ijet and that's where it will get captured. There are countries in the world who can't use Amex for whatever reason and they would book direct, and that's where some of these things fall down, where people can book a flight direct with an airline or through Expedia or something like that because it's cheaper. So that is part of getting that written into a policy that states you must book via this TMC, Travel Management Company.

RL: And if they do that through another company are they forced to notify Ijet? Is it compulsory to notify Ijet?

P2: No it's not, it's not written in policy. There is an option to allow us to manually input a trip so if I booked a flight direct then I can manually put my trip into Ijet but it is not compulsory.

RL: Ok when we look at the training, Ijet i have heard, will supply you, the minute you say you are going to a high risk location, they will give you a sort of form, of briefing that you can read through highlighting the generic security concerns and things like that. Is that correct?

P2: Yes so if there is civil unrest there is a generic brief for civil unrest, if there is terrorism then there is a generic brief for that, but there is also a in Country or City specific brief as well so each Country and City has got a travel brief as well which will highlight any security issues, it will highlight the recent alerts in that Country, if there has been any. Yes, it's a pretty good system.

RL: With using a company like Ijet do they look at your organisational context much, for example do they look at, if you are a company supplying engineers to go work abroad or if you have got a company full of computer programmers who take in sensitive data, do they look into that much?

P2: Not in my experience no. I suppose the only difference is, is that you can give travellers a hierarchy, so you have got your standard travellers, you have got your expats that are on a long term assignment somewhere and may have family and dependants and you can assign a VIP status to someone as well so, obviously it speaks for itself. Apart from that there is nothing around specific roles really that would come under us I suppose. So if we had some IT technical people who needed to get into Russia and take a load of laptops with them then that's going to be more of a problem than someone saying they are marketing executive or something but that would come under us rather than Ijet.

RL: Ok, security awareness training. Do you do any specific security training?

P2: Only if we are asked, it's more around expats so if someone is going on long term assignment somewhere like Johannesburg for example for us we would do a brief with them, a face to face brief on what you should and shouldn't do and then we may arrange for either us or someone in country to do a risk assessment of their home and their travel plans and things like that, but in terms of your generic travellers we don't. We have spoken about doing a computer based training an online package where it just might highlight some of the things that you should and shouldn't do and just the basic stuff really.

RL: And never to the extent of anything like HEAT training and CONDO training, what they give to journalists?

P2: No, we don't go to that many locations which require it but saying that all the emerging markets are in the high risk countries at the moment and we are starting to branch more into mid Africa and places like that which potentially could change things a little bit I think.

RL: In your organisation or experience what other counter measures do you use to manage this risk apart from the ones we have discussed?

P2: So in terms of what?

RL: So in terms of the ways you would transfer the risk, avoid the risk, the ways to reduce the risk?

P2: So, for example, somewhere like Ukraine at the moment we have just decided not to travel, so it is quite easy, let's not try and manage the risk, we've just decided not to travel at the moment so I suppose that's a fairly easy one. If we were going to go to somewhere like Lagos or maybe Nairobi at the moment, then we may arrange ground support so we will use a third party company to provide that service that meet and greet or depending on the level it may be EP or whatever but for us that is pretty rare to be honest. We've got quite a big business in Brazil which we use an approved car service, it's literally pick up from the airport and drop off. We don't supply the EP element that much. In terms of other counter measures.

RL: Specialist insurance?

P2: All our employees have travel insurance, there may be other types of insurance that we shouldn't really talk about.

RL: Like kidnap and ransom, things like that?

P2: Yes possibly there may be that type of insurance as well.

RL: So under avoidance you have quite regularly refused travel to high risk locations. Do you limit and restrict passenger numbers when people travel off to conferences etc.?

P2: We try to but financially the more people you put on a specific aeroplane the cheaper the seats become unfortunately. We have an unwritten rule of 25 or over is too many, to keep it below that, we also try to restrict the exec's travelling all on the same plane or whatever just in case something happens but it is not enforced as well as it probably could be.

RL: There is no specific policy, that's not part of any policy?

P2: No, no.

RL: Looking at emergency contacts is that done through Ijet or is that done in house where one of your workers gets into trouble?

P2: We have a global emergency line which any employee can call. It is managed by a third party, Ijet actually, but that can be any type of risk it doesn't have to be a travel risk it can be a car accident or if someone loses their laptop or a medical whatever they can just ring that number and they will get re-directed to whoever they need to.

RL: Security updates you said that you are in the process of setting up the website, are there any sort of technological things that you have got, apps for people's phones?

P2: No, we have no travel trackers or anything like that. Ijet allows you to monitor personnel. So we can log onto Ijet today and I can see exactly where people have travelled to globally, but in terms of real time tracking, there is nothing that we have got. If we needed to contact someone then if it's a small number then we would ring them or email or text something like that. Failing that if it's a large group of people then we have got a Imodus that we can push out business alerts to make contact with us or we can push out a conference call number for a certain time, everyone can just jump on that and we can brief them on what the issue is or failing that if we have a business in that particular location we can obviously contact the staff to go and check on someone at the hotel or we can contact a security provider in Country and get them to go and do

it for us, but there are no trackers or apps where people have to report in or anything like that.

RL: And the Ijet information is that pushed to you and then you push it to the travellers or is that done directly from Ijet to the travellers?

P2: Any alerts are real time to travellers, so if something happens in London now then any travellers in London will see that alert automatically, we don't have to start that process. If we hear something via, twitter is normally quicker than anything else at the moment then we would reach out to the travellers direct and check that everything is ok if there are any issues.

RL: So Ijet maybe do the briefing prior to the trip?

P2: Yes but there are real time alerts as well, so if something happens now then that alert automatically goes to any travellers that are in that Country.

RL: Via email?

P2: Via email yes.

RL: Are there then emergency and crisis response teams?

P2: Yes, so if it is a physical security issue, travel security issue then that would come under our team but with input from the Global Business Continuity office as well, so it sits in the same department as us so they generally manage the incident and we feed into the subject matter experts I suppose for travel security or whatever.

RL: So global security would take the lead?

P2: Yes

RL: And then HR, everybody else?

P2: Yes so depending how big an issue it is then yes we would call on the other departments, whoever should be involved, so yes if it HR, if it should be facilities, if its building related as well, could be Legal, could be internal communication, press, whatever.

RL: In your organisation is the effectiveness of your travel risk programme evaluated, do you evaluate what you have put in place?

P2: We self-evaluate as one does, because we are pretty critical of ourselves, so I suppose there is that constant battle. I think, you know it is one of those hot potatoes particularly at the moment, travel security, and it gets scrutinised by the business an awful lot because if we are travelling to what we perceive to be a high risk country, locals in country may not think it is high risk. So I think somewhere like Johannesburg is a fairly good example you know locals would consider Johannesburg to be fine whereas for some reason we get really scared about Johannesburg and recommend all these measures which someone has to pay for at the end of the day. So i think there is that business scrutinisation as well, and then good old internal audit. We are actually going through an internal audit at the moment against physical security, and travel security is part of that so they will audit our processes and procedures that are in place and whether or not they are effective really.

RL: Things like debriefing, surveying of personnel, is that done, sort of to try to see where there have been, incidents, where there have been problems, to see how people are feeling, if they feel safe about business travel?

P2: No we don't do that proactively. We wouldn't necessarily contact someone who has just travelled somewhere and just say to them, how did it all go, is there anything we can improve, we wouldn't do that. If there was an incident then there would be that follow up and there would be an internal investigation and lessons learnt and everything like that, but in terms of being more proactive we don't do that.

RL: Analysis of KPI's, looking on return on investment, and money you have spent on all these measures, the training, is there analysis done into the number of incidents that have been reduced, the amount of calls received/reduced, the use of Ijet?

P2: We get very few incidents, really very few, the incidents that we get are more sort of medical related or lost laptops and things like that. In terms of what I class as travel security issues it is really few. There are no real KPI's monitoring return on investment and things like that. I suppose if we sent an employee somewhere where we did have to provide an enhanced level of security then we would always follow up with that person afterwards to check that everything went ok, and how was the security company that we used and things like that but that is pretty rare to be honest.

RL: Would the reason for that be the cost involved and the time and the manpower, or is it just seen that you will only ever analyse things when you've have had an issue and then you think, oh where did we go wrong? Would it be because it is just difficult to do, it's time consuming and costs a lot?

P2: Yes I think time consuming especially and that comes down to resources then. And then I suppose who maybe should do it. Should we do it, or would it be a third party internally that would do it. It is an interesting thing, the only thing loosely that we do follow up on is any security service that we arrange in Country or if we arrange a car service or something like that we send the traveller a survey afterwards just to give us a feeling on how that service went, just so that if the company is no good then obviously we can strike them off our preferred suppliers list basically.

RL: My final question was just to find out, if you have ever had to deal with any serious security incidents involving your business travellers?

P2: Personally no, as I say, touch wood we have been pretty good, we don't go to any massively high risk Countries but then someone can come to London and get themselves into trouble pretty easily can't they? No we have had nothing and nothing that I can think of from another region's point of view either.

RL: Lastly, any comments or questions?

P2: No

Appendix 10.

Transcription Interview Three

Interview 3
03/06/14
15:37

RL: Before we begin any comments or questions?

P3: No

RL: The first aspect I am looking at is in the strategic manner in which business travel security risk is managed. In your experience who would you say are the key stakeholders that are involved in the practice?

P3: It would be corporate security or loss prevention and a travel manager, and this is a little bit of the context, so we are like a subsidiary here of a US company so we've got obviously travellers of every nationality based in London travelling virtually all over the Globe but some of our actual corporate policies are set in the US.

RL: Yes

P3: So, for example, there is a travel manager in the US who would say they have global responsibility but then when it comes to travel security briefings and anything like that for any of the London based people then that is my responsibility.

RL: So would you say the risk owner would be yourself or the travel manager in the States?

P3: I think it would be the travel manager in the States ultimately, I suppose you would call it a partnership amongst a couple of departments.

RL: Yes, but the travel manager rather than corporate security taking the lead as the risk owner, the travel manager?

P3: Do you mean all of the risk as just travel risk?

RL: The travel security risks.

P3: No then that would be corporate security or loss prevention.

RL: Corporate security falling to yourself?

P3: Yes

RL: In the organisation how would you say the responsibility is shared between the traveller and the organisation? Is it seen as a 50/50 split? Is it seen that the organisation is to do the majority of the work, the travellers must comply? How would you say, if not in this business, in your experience?

P3: Let me break that down, I would say it probably is 50/50 so we provide the services and any background information etc. to the location that they are travelling in. But when travellers make routine bookings, like I am sure many other companies, it is their responsibility to actually download the information for the particular area that they are going to so there is a lot of responsibility on the traveller. We provide access to a travel risk management programme and when they make a booking they are supposed to take all the information, or retrieve the information, for the location they are going to, know of any risks etc. So we provide briefings and trainings generally across the office and we promote the use of an app, as an example, but again if the traveller doesn't download it how do they know about the risks.

RL: Exactly. They are very much shared?

P3: Yes

RL: Would you say, it's corporate security yourself that's involved and the travel manager, would you say there is any other functional group, HR, Legal, any other senior managers that are more suited to this role?

P3: An interesting thing about that is, and again I will reference this company in particular, the elements have various insurance policies and things for travellers which sit aside or alongside all other type of risk management insurance policies, so, interestingly, when I have been doing travel security briefings HR kind of insist to come along and they use that as their platform to brief the staff on what they are, you know, support from an HR point of view in relation to insurance policies and if things go wrong so more mundane things probably, so they just lose their luggage or is something fairly minor happens their covered on insurance for that so that becomes a bit of a partnership. Whether or not I would like them to be seen to be taking the lead I suppose I would have no real strong opinion either way because I think if they were the lead then I would still, I would be using their meetings as the platform to download my security advice then.

RL: Moving now onto the operational aspects of managing the risk, how are business travel security risks assessed?

P3: It's majority out sourced basically. We use that to a large degree to assess the risks, then if particular countries or areas become more high risk then we would have a more in depth conversation, probably with the third party provider. For example the Ukraine and things like that, when that kicks off, then we will just have additional meetings and make a decision on whether or not we actually want people to travel. Some organisations the travel is so fundamental to what you are actually as an organisation, I am guessing some organisations just can't stop travellers but mostly we are in a situation where actually if we just holt travel it's not going to cost a business continuity issue or there should be no major repercussions for it so we tend to operate cautiously like that and if something is happening in a particular Country we just ban travel to it.

RL: Ok. The third party provider that you use is this basically a travel management company that looks at the itineraries and the expenses side of things, is it a specialist

security and medical advice company or is it a technological provider who provide the apps and things like Concur and companies like that?

P3: It's medical and security advice.

RL: Ok and this is a continuous function, you've got them on the books you work with them permanently?

P3: Yes

RL: So continuous rolling contract?

P3: Yes

RL: All the employees?

P3: Yes everybody who travels has access to it and every time they book they get a reminder of what website to look onto and a reminder about the app. And yes it's a continuous process.

RL: Ok. How are the identified security risks promulgated to personnel?

P3: Again I would say most of the countries we travel to are generally low or medium risk so again the risks for the particular country come when the traveller makes the booking then if there is any particular issue in that country we get informed of that at the time. They always get told to check various websites and the Foreign Commonwealth Office again so that's a bit back to your first question that we do ask them to do other work themselves but then with our relationship with the travel company as well as the risk of you going up the scale to medium to high and to high risk locations then that's when we would step in and make that decision to ban travel.

RL: Ok. Do you have a specific travel security policy?

P3: No

RL: Do travel security risks fall under another policy?

P3: I think there is kind of advice, whether or not you would call it an actual policy, I don't think so. It's documented as a policy I think for certain criteria and briefings etc., which you could technically argue is policy, but it's not actually called that it's called travel advice.

RL: Ok. Measures such as having a compulsory pre-trip authorisation procedure, do you have that in place?

P3: Only in high risk locations.

RL: Can people make bookings outside of your usual travel management company? Can people make private bookings and travel on those private bookings?

P3: Well they could do, yes they could do.

RL: And is there anything in place to force them, I know you said it's a joint responsibility for people to, but is there anything in place which is compulsory for them to notify the relevant department to say I am travelling to so and so?

P3: You mean for work?

RL: Yes

P3: The policy officially is that they must use the travel booking company for all travel so we would obviously pick up that and let's say, for example, somebody tried to book a trip to Ukraine we will have briefed the travel company to say no travel to Ukraine. If anyone contacts you wishing to make a booking to that country then you must contact this person and we determine who that is. But then going back to your point. Actually they could just go outside the travel company and make travel arrangements and if they chose not to tell anyone within the company then we wouldn't know, but we certainly make this strong advice or policy that they must book all travel through the company.

RL: When it comes to training obviously the travel management company provides that pre-trip advisory giving people the necessary information they may need. Do you do any general security awareness training or provide any specialist security training?

P3: Yes I provide general security awareness sessions just normal security advice for travellers and that's when I also promote that they should download the app, look at the websites before you go and inform them of their obligations as well.

RL: You said that you have got no travel to high risk locations so is there no need for specialised training, sort of what the journalists do with their HEAT and CONDO training?

P3: No, it's not that environment.

RL: Can you tell me if there is any other counter measures that you use within the organisation to manage the risk, other things such as the transference, avoidance and reduction methods?

P3: Not really, i think with VIP travel to a medium to high risk area that we thought had to go ahead we would use private security companies for close protection and things like that, that would be the main other thing that we would do, I think we would just ban travel really.

RL: And for people going abroad is there general insurance for travellers and then are there also specific measures like kidnap and ransom insurance which you would have for people, is that also in place?

P3: Yes

RL: Refusal to travel you have covered that. Do you limit passenger numbers and restrict groups?

P3: Yes that is covered in our travel policy, it's restricted on total number of travel and also the level of job role within the organisation the maximum number of people that can travel on the same flight for example and things like that.

RL: Emergency contacts is that done in house or it's done through your third party provider.

P3: It's through a third party.

RL: And then security updates for the travellers is that done by the third party or pushed from yourself or from the company?

P3: That's pushed from third party as well and obviously with the app if the traveller has downloaded it they get 24 hour reports on the location that they are in so they can just click on it and it will give them latest alerts for my location if they check that that is how they can pull it down as well.

RL: And does that app provide the facility for traveller tracking as well?

P3: No it doesn't.

RL: Is that something that you would consider using?

P3: We haven't really considered it, or at least I haven't, certainly from the European arm of things. I would imagine in the US it's probably on privacy reasons why we don't do it, and again there are no real high risk locations involved.

RL: Emergency and crisis response teams do you have those in place?

P3: Yes, how we do it here is we kind of double up on the business continuity management so we have a system for business continuity and we double that up on crisis management so it's the same key leaders within the business or in that theme. It's effectively a crisis management team. So yes we have all that.

RL: And which department takes the lead in that?

P3: For the crisis management?

RL: Yes

P3: The actual figure head is the Managing Director for Europe and I'm officially the deputy which I think is really a joint approach because I think they are looking to me for the security advice and everything whether that be an incident for example in London or it's an international traveller, or whatever but it's a combination of the two of us really.

RL: When it comes to evaluating the effectiveness of your programme, is it evaluated, the effectiveness of it?

P3: I am not aware of any evaluation, no, other than the performance of the third party. You know, do we think we are getting up to date information from them and are they providing a good service, but I am not aware of any full evaluation.

RL: Things like analysing key performance indicators, return on investment, looking at insurance premiums before and after?

P3: No I am not aware of any of that.

RL: Are any interviews or observations done on traveller behaviour? Sort of surveys, questionnaires done maybe after people have travelled to find out if they have had issues, had problems, how have they found the third party provider to be, the services rendered?

P3: I think we do that informally. It's something I have certainly been considering here in London primarily because of all the variety of various nationalities now resident and living, working in London, but then travelling all over the world but they are UK employees so therefore UK duty of care and all that, so it's something I have been considering, but at the moment it would be kind of informal where I would know who

is travelling a lot for example, and I would just go and ask them how have you found the service that's provided, have you had to use them, what do you think of it, just informal stuff really.

RL: And the training that you give do you sort of test people pre-training/post training to measure the improvement and knowledge?

P3: No it's pretty much an awareness session really.

RL: And my last question, have you dealt with any serious security incidents relating to business travel and if so how did you manage it, how did you approach it?

P3: No we haven't had to maybe some of that is the cautious approach that we have where we step in and ban the travel if it looks like any events are coming to the fore. I am trying to think of any media events that were non security related, I can't, minor things when the ice cloud occurred with people stranded in various places and their running out of cash and things like that, but that was all dealt with individually. We have had no pure security incidents at the minute.

RL: That's very good news let's hope it stays that way

P3: Exactly

RL: Any comments or questions?

P3: No I don't think so, have you anything else

RL: No thanks you have answered all the questions that I need.