



University of Warwick institutional repository: <http://go.warwick.ac.uk/wrap>

This paper is made available online in accordance with publisher policies. Please scroll down to view the document itself. Please refer to the repository record for this item and our policy information available from the repository home page for further information.

To see the final version of this paper please visit the publisher's website. Access to the published version may require a subscription.

Author(s): Bridgette Sullivan-Taylor and David Wilson

Article Title: Managing the Threat of Terrorism in British Travel and Leisure Organizations

Year of publication: 2009

Link to published article:

<http://dx.doi.org/10.1177/0170840608101480>

Publisher statement: © Organization Studies, February/March 2009  
vol. 30 no. 2-3 251-276. Published by Sage Publications Ltd.

## **Confirmation**

This paper is not currently under review, accepted, and/or being published by any other journal at the time of this submission.

### **Author Bios:**

Bridgette Sullivan-Taylor is an Assistant Professor of Strategy and Organisation at Warwick Business School. She has previously held management positions in both private and public sector organizations in New Zealand and the UK. She has also held academic appointments in the UK, Belgium, New Zealand and Switzerland. She is currently the Director of the Strategy and Organisational Learning and Resilience Unit at Warwick Business School and is a member of EGOS, BAM, AIB and SMS where she has been elected as 'Rep-at-Large for the Strategic Management Society Global Strategy Group. Her current research interests include globalization, internationalization processes, the strategic management implications of global terrorism, managing risk and uncertainty; strategic change, innovation and knowledge management transfer processes, organizational learning and the development of communities of practices in inter-organizational relationships.

David Wilson is Professor of Strategy and Organization at the University of Warwick Business School, where he is currently Deputy Dean. He is an ex-Chair of the European Group for Organization Studies (EGOS) and the British Academy of Management. He is also a past Editor-in-Chief of Organization Studies (OS) and is currently Chair of the Advisory Board (OS) and an elected member of the EGOS Board. His research interests include strategy, decision making, performance and power in organizations.

**Organization Studies**  
**Special Issue**  
**on**  
**"Organizations and Risk in Late Modernity"**

---

**Title:**

Managing the Threat of Terrorism in British Travel and Leisure  
Organizations

**Authors:**

Dr Bridgette Sullivan-Taylor  
Assistant Professor of Strategy and Organisation  
MSM Group  
Warwick Business School  
University of Warwick  
CV4 7AL  
UK  
Ph: 024 765 74163  
Fax: 024 765 24628  
Email: [Bridgette.Sullivan-Taylor@wbs.ac.uk](mailto:Bridgette.Sullivan-Taylor@wbs.ac.uk)

Professor David C. Wilson  
Deputy Dean  
Warwick Business School  
University of Warwick  
CV4 7AL  
UK

Email: [David.Wilson@wbs.ac.uk](mailto:David.Wilson@wbs.ac.uk)

This research was supported by Leverhulme Grant no: ECF/2004/0386

Thanks are due to Max Boisot, Joe Lampel, Bill McKelvey, Jamal Shamsie and Zur Shapira for their comments on an earlier draft of this paper.

**Title:**

Managing the Threat of Terrorism in British Travel and Leisure  
Organizations

**Key words:**

Uncertainty, risk and extreme threats, managerial perceptions, terrorism, agency and organization.

## **ABSTRACT**

This paper examines the perceived threats from terrorism in six organizations in the travel and leisure sector in the UK. These organizations are particularly exposed to such extreme threats. This paper examines how managers in organizations deal with uncertainty where probabilities are impossible or difficult to define and examines how they face the challenge of interpreting and acting upon these interpretations. Theoretically the paper draws upon two lenses: organizational resilience and institutional perspectives. The former assumes managers can act autonomously to increase organizational resilience. The latter argues that systemic features of organization are more accurate explanations of why managers and organizations fail to spot threats and impending disasters. The data indicate that perceptions of uncertainty and threats from terrorism and theories of action differ in and between organizations depending upon factors such as the accuracy and completeness of information; previous experience of terrorist events and whether or not these threats were prioritized over other uncertainties. Three organizations in the aviation industry prioritize threats from terrorism, whilst three organizations in the leisure and travel sector do not. Managers in the aviation industry tend to take a proactive, organizational resilience stance toward uncertainty, whilst managers in the other organizations are more reactive, or take little action, with systemic features of organization taking precedence over decisions and actions.

## **INTRODUCTION**

This paper examines how the threats of terrorism are being handled in a range of UK firms in the Travel and Leisure Sector (TLS) in the UK in the post 9/11 era. We examine how managers perceive these threats and how they justify their actions in securing defences against possible attack. We examine how and why these perceptions and actions vary across the six organizations studied.

We argue that the threat of terrorism represents what Meyer (1982) termed an example of ‘hyperturbulence’, or quantum change to the status quo. Typically, researchers have examined such quantum changes in terms of shifting industry boundaries, technological revolutions and new forms of organization (Meyer, Gaba and Colwell 2005). These quantum changes are associated with high risk. In this study, we argue that the threat of terrorism represents a similar degree of risk which is likely to necessitate profound changes to everyday organization practices. To do this, we examine data from six TLS organizations in the UK.

We chose the post 9/11 era to conduct this research, since that single event marks what Meyer (1982) termed an 'exogenous jolt'. There have been a number of other such jolts. These include the bombing of Bali, Madrid, London, Egypt and Turkey; the hijacking of an outbound flight from Moscow airport in 2004 and major disruptions to international flights and travellers caused by airlines and airports trying to contain the threat of terrorism. We further argue that following these jolts, it would be reasonable to expect some evidence of commensurate management action in organizations exposed to such threats (and acts) of terrorism. This is an important question, since many organization theorists have argued that, in general, managers will adopt routine and institutionalized adjustments to such jolts, rather than embark upon more radical changes (Greenwood and Hinings 1988). March (1981) has similarly argued that organizations are likely to adopt incremental adjustments and routine changes in the face of both continuous and discontinuous changes (jolts encouraging discontinuous change). We will examine whether or not this is the case in the organizations we studied.

Uncertainty and risk are no strangers to organization theory. However, the majority of theorists advocate adopting strategies to preserve equilibrium and linearity in the face of uncertainties by posing uncertainties as a variety of assessable risks (see Meyer, Gaba and Colwell 1985: 456). For example, Thompson (1967) argued that above all else, the technical core of an organization should be protected from uncertainty by creating boundary-spanning departments which could buffer the organization's transformational or production processes. The heart of the organization could be shielded from potentially damaging shocks and buffering could provide stability and continuity by helping reduce exposure to threat. Bryan and Joyce (2005) take a similar stance, arguing that although the technical core of the organization is now mostly professional staff (rather than technical), organizational designs and architectures should similarly protect them from unnecessary risks.

Knight (1921) and Keynes (1921) describe risk as a situation when the probabilities describing unknown events are calculable, whilst uncertainty obtains when probabilities are unknown, either in the absence of prior experience, or because we do not know which probability distribution to use from a number of possible options. In organization theory this is often called ambiguity, or decision making under complete ignorance.

We argue that the threat of terrorism goes beyond conventional notions of risk, taking organizations into the arena of high uncertainty (defining risk is measurable; uncertainty is not), although Beck (1992: 26) has argued that risks have also changed in nature, *'they have become more global, less readily identifiable, more problematic, less easily managed, and they are more anxiety provoking'*. (Beck, 1992: 26), so the line between risk and uncertainty is becoming increasingly blurred. The threat of global terrorism fits with Beck's perspective. Terrorist related uncertainties have parallels with other 'bolts out of the blue' such as 'normal' accidents (Perrow 1999, e.g. Bhopal) man-made disasters (Turner 1976, e.g. Columbia) or natural disasters (Lynch 2004, e.g. South East Asia tsunami, Hurricane Katrina). Following Czinkota et al. (2004: 589) we define terrorism as:

*The threat or use of violence to attain political or other goals through intimidation (threatened or actual) towards organizations and individuals in civil society.*

To date, little empirical research has been conducted into how managers deal with uncertainties created by the threat (and sometimes the actuality) of terrorist attacks (exceptions include Cornish 2007; Sullivan-Taylor and Wilson 2007). Czinkota et al. (2005: 583) argue that conceptual and empirical research on possible relationships between terrorism and management are missing from the literature. We know very little about how managers make decisions about the perceived threat of terrorism (Faulkner 2001). This paper attempts to throw some light on these processes.

In particular, we investigate how managers interpret the threat of terrorism and what theories of action managers take toward acting upon such uncertainties. Theories of action arise from managers mapping their environments and from inferring both causal arguments about assumed relationships between events and also formulating what action to take. Finally, we attempt to explain why managers perceive and act in the ways they do towards this particular set of uncertainties.

### **Situating the Research Theoretically**

There are at least two broad and contradictory theoretical orientations drawn from organization theory which can be applied to this field of study. These are termed here, the organizational resilience approach (which gives primacy to managerial agency) and a more institutionalist perspective (which gives primacy to the social structures and embedded processes of organization).



Theorists espousing the resilience approach have based much of their work on Weick and Sutcliffe's (2001) notion of high reliability organizations (those which prosper and succeed in high-risk industries). Hamel and Valikangas (2003) argue that a highly resilient company has the power to prosper no matter what is the nature of the uncertainties it faces. Resilient companies meticulously prepare for the worst and establish routines enabling them to improvise rapid responses to crises. Weick and Sutcliffe (2001) argue that HROs exhibit mindfulness, meaning a combination of high alertness, flexibility, and adaptability which, in turn, lead to increased resilience. In summary, HROs are never tricked by their successes, paying detailed attention to even small failures instead; they listen to their experts on the front line and not just senior managers; they let unexpected circumstances provide solutions; and they embrace complexity and anticipate. HROs also think strategically by acting and learning from those actions (rather than adopting a grand strategy of first think, then act). As Weick and Sutcliffe (2001) argue, actions by managers can build an organizational capacity for resilience:

- **Technical:** the ability of managers to ensure that organizational systems perform to high levels when subject to extreme stress
- **Organizational:** the preparedness of managers to make decisions (however counter-intuitive these might sound initially) and to take actions to reduce disaster vulnerability and impacts
- **Resourcefulness:** the capacity of managers to identify potential problems, establish priorities and mobilize resources to avoid damage or disruption
- **Rapidity:** the capacity of managers to make decisions on threats (e.g. from terrorism) without undue delay.

The 'resilience' perspective has gained ground in the last few years as a solution to organizations facing high levels of threat in all aspects of their operating environment. In the military and security sectors, building and maintaining resilience has become a by-word for significantly increased safety (see Cornish 2007). These writers emphasize the need for organizations to develop the ability to bounce back and self-right following a crisis. An important aspect concerns the impact of terrorist threats on people individually (as well as the organization itself) necessitating a shift from a reactive to a proactive stance toward crisis management and disaster recovery. Scenario planning and worst-case scenarios are part of this approach. Anticipation is key (Wensley 2003). The preparedness of an organization (via its managers) to assess and face future threats is crucial. Organizations which are not resilient are likely to be vulnerable, exposed and, perhaps, complacent toward the threats and hazards they face (Omand 2006).

This essentially resource-based view has extended beyond security and has permeated management thinking toward uncertainty, especially in the area of strategic management. Hamel and Valikangas (2003), for example, discuss the ‘threat’ of existing business models being considered (erroneously) immortal and extend the resilience argument to include organizational strategy more generally, using many of the same concepts developed in the military and security-related texts (such as anticipating extreme events through worst-case scenarios; avoiding nostalgia and arrogance traps such as assuming an organization will always be the market leader). In line with much popular management literature, Hamel and Valikangas (2003) view such concepts as organizational learning, experimentation and information technology as effective counter-terrorist and resilience building blocks. Resilience has permeated other areas such as trust (Bhide and Stevenson, 1992), leadership (Fiedler and Garcia, 1987) and the personal qualities of employees (Furnham, 1992). Overall, in all of these approaches lies an abiding belief in the voluntaristic abilities and facilities of managerial agency. That managers can build resilient organizations is the leitmotiv of many articles in these areas. The agency debate has also permeated the field of Sociology in examining risk. Cerulo (2007: 5), for example, argues that planning for worst-case scenarios can be very helpful in building resilience, adding that the majority of individual managers tend to adopt an overly optimistic view of risk, a concept she terms ‘positive asymmetry’ (Cerulo 2007: 17).

Running counter to the above arguments lies a group of more deterministic, more organizational-institutionalist perspectives and arguments (Gephart, 2004), which demote the importance and influence of individual agency in favour of more exogenous explanations of managerial action (or inaction).

Perrow (1984) analyzed a range of disasters including nuclear incidents, and accidents in petrochemical plants and organizations ranging from space flight to genetic engineering. Subsequent disasters included Chernobyl, Bhopal, and the Challenger explosion. Reviewing these disasters, Starbuck and Farjoun (2005) concluded that the sources of disasters were more organizational in origin than they were a function of managerial action. Both the Challenger and the Columbia Space Shuttle ‘accidents’ arose from the:

*‘innate, essential, intrinsic, and real nature of NASA’s organizational system:  
a complex constellation of interacting factors that included NASA’s  
political/economic environment, organization structure, and layered cultures*

*that affected how people making technical decisions defined and redefined risk'*

(Vaughan 2005:85).

In other words, the roots of these failures were organizational in nature. Several authors researching the tourist industry report similar findings of organizationally based failures including a general lack of innovation and an over-reliance on old and familiar ways in the face of these specific risks (Faulkner 2001; Tarlow and Santana 2002). Czinkota et al. (2005) argued that in *'the USA the majority of organizations are unprepared to meet such risks and that complacency has set in'* (Czinkota et al. 2005: 588).

This unpreparedness emphasizes institutionally bound explanations (such as an over-reliance on technical or administrative systems to provide an accurate guide to action). For example, Hedberg (1981) and Weick (1995) infer that exposure to new, risky situations increases uncertainty and forces managers to seek new theories of action. However, as Weick (1995) observes, theories of action may simply involve managers looking to the past, making sense of new threats in much the same ways as they made sense of old and more familiar threats, thereby treating decisions on terrorism threat in much the same ways as they handle other decisions. The norms and values of decision making in organizations (well understood and familiar organizationally institutionalized processes) take priority of explanation over individual action.

One of the most recent authors to embrace this systemic view specifically in the field of threats from terrorism is Taleb (2007). He argues that individuals are good at retrospectively 'predicting' random events that happened in the past, but find looking forward impossible. Largely this is because, on the basis of limited experience (these managers are unlikely to have experienced a terrorist attack directly) they conclude that such attacks are highly improbable (they won't happen to their organization). Taleb argues that organizational history reveals much about the ways in which the construction of elegant chains of reasoning is a feature of the historical narrative, presenting neatness and order (when there was little) and causation (when events may have been random). From this perspective, history (and by implication organizational stories) as well as management actions become institutionalized. Taleb (2007: 15) calls this 'retrospective distortion'.

From this perspective, features of the institution (its history, for example) shape both managerial perception and action. Although managers may have to refine theories of action as new situations

are encountered (Hedberg 1981; Laqueur 1999), such change and refinement is likely to be slow and incremental (Turner 1976; Weick 1995) because of institutional inertia. Turner (1976) argues that organizations adopt strong rigidities in their institutional beliefs that prevent them from handling risks from disasters effectively and from this institutional perspective the same may be argued about organizational responses to terrorism. Such arguments have been well rehearsed elsewhere in organization theory (see, for example, Di Maggio and Powell, 1983; March and Olsen 1984; Powell and Di Maggio 1991; Scott 2001) but they have resonance with the subject of this paper.

The institutional perspective gives primacy to the roles of structures, rules, norms, and routines, as they become established as authoritative guidelines for social behaviours in organizations. As Scott (2001: 48) argues:

*“[organizations] are composed of cultural-cognitive, normative, and regulative elements that, together with associated activities and resources, provide stability and meaning to social life. Institutions are transmitted by various types of carriers, including symbolic systems, relational systems, routines, and artefacts”.*

This is precisely Taleb’s (2007) argument. Embedded assumptions represent a potentially dangerous asymmetry of both perception and response (it won’t happen to us; we need not take any actions against the threat). So how does this institutional perspective impact upon understanding and interpreting how managers act under the threat of terrorism? First, it adopts a sceptical position toward viewing managers as rational individual actors, arguing instead that managers’ perceptions and actions will inevitably be shaped by institutional variables. Secondly, it argues that relatively rare events (such as the act of terrorism) rarely occur within a normal distribution of probability. Yet organizations strive in the design of their structures and processes toward rationality in assuming that threats can be interpreted within the realm of calculable odds which are, hence, likely to occur within a normal distribution (see Taleb 2007). These institutional pressures force managers to adopt what Taleb (2007: 25) calls the ‘ludic fallacy’ (assuming that all odds are calculable). From this perspective, the odds of a terrorist attack are likely to be dealt with using the same (normal distribution) criteria which might be applied to, say, decisions to invest or to change key suppliers.

Whilst theoretically diverse, the resilience and institutional perspectives share a common feature, that of managerial action. If research can delineate what ‘frames of reference’ managers embrace in guiding their actions or framing their decisions on the threat of terrorism, it should be able to reveal the extent to which such actions and framing are more a function of managerial actions to build organizational resilience, or are more institutionally bounded (Orlikowski and Gash 1994). That is a central purpose of this paper.

## **Sample**

All six organizations are in the travel and leisure sector (TLS). Such organizations are relatively highly exposed to threats from terrorist threats and actions. As Czinkota, et al (2005) observe, terrorism has directly affected the fortunes of organizations in this sector and, as Mayntz (2004) explains, terrorism is a relatively new threat and such organizations are often a primary target for terrorist threats. Other authors have also shown how exposed the TLS is to terrorism (see, for example, Bentley and Page 2001; Callander and Page 2003; Greenaway 1996). All the sample organizations are based in the UK and operate internationally (see Table I for a summary of the sample).

Gaining quality access to organizations is difficult on most occasions, but is especially so when the topic is often perceived by informants to be how well (or how badly) managers cope with the threat of terrorism. There was reluctance amongst many organizations to allow access for this study. The six organizations studied here therefore represent those which would allow quality access. We were helped in gaining access to the first organization by its CEO being an alumnus of the University. Access to further organizations was gained by a ‘rolling’ process whereby organizations granting access were asked to recommend others, so as to enable us to compare our findings across different TLS firms. As an unintended consequence, this gave us a range of organizations linked along a supply chain which involves attracting, organizing and transporting visitors into a country, processing and transporting them internally to the city and venue of their final destination. This may be a holiday or an event such as the Chelsea Flower Show, an exhibition or a sporting event such as Wimbledon Tennis or the 2012 Olympics. The sample for this research therefore comprises organizations interlinked within what is termed the UK’s ‘visitor economy’. Paraskevas and Arendell (2007) advocate that TLS organisations within the visitor

economy can and should play an active role in the co-ordination of tourism stakeholders in addressing the threat of terrorism.

A further reason for choosing to study organizations in this sector is that they have recently become the focus of regulation specifically concerned with the threat of terrorism. For example, the UK Government's Civil Contingencies Act 2004 requires private sector organizations to have inter-organizational emergency response and recovery plans and VisitBritain (previously UK Tourism and the British Tourism Authority) requires organizations in the travel and leisure sector to formalize their business continuity plans and to be clear about their responses to the threat or act of a terrorist attack.

A theoretical sampling framework was used since we picked a sector which is particularly exposed to terrorism and the managers we interviewed were those who might be expected to be responsible for their organization's responses and actions toward the threat of terrorism.

---

TABLE I ABOUT HERE

---

## **Method**

Qualitative research has previously been conducted to investigate infrequent organizational events, such as accidents and disasters. Studies by Gephart (1984 and 1988b), Meyer (1982), Roberts (1990), and Vaughan (1990), for example, have produced case descriptions of disasters and responses to environmental jolts. These studies have also provided insights that have established organizational disasters as important topics for management research. To further develop this area, Gephart (1993: 1467) argued that *'disaster studies and management research could benefit from a more extensive development and systematic, exhaustive analyses of comprehensive qualitative data bases'*. This paper provides qualitative research that helps to address this call. This research was an exploratory examination of how managers perceive and act upon uncertainty in the context of terrorist threats. Hence, a qualitative, semi-grounded and inductive approach was adopted (Van Maanen 1983; Glaser and Strauss 1967: 3).

All data were collected using in-depth interviews with key informants in each organization. All discussions and interviews were digitally recorded. Multiple informants were drawn from the sample organizations (ranging from a minimum of three to a maximum of five per organization). All informants were closely involved in both assessing and in taking strategic decisions about threats facing their organization and this was a criterion for their selection as key informants. Interviews typically lasted two hours and in some cases substantially longer (where the researchers were able to set up group discussions with key informants which often lasted up to half a day). Three organizations were the site for group discussions (Catering Supplier; Airport; Tour Company). Typically, informants would bring along two or three other managers to the group discussions to comment and give more detailed information. These discussions were in addition to the in-depth interviews carried out with individual informants. It was not possible to organize these group discussions in every case, but this data collection method was used where it was possible to get a small group of around six people together at the same time for half a day. Appendix A gives examples of questions and prompts used during interviews and group discussions.

Data collection spanned a nine-month period between January and September 2004. Table II summarises informants, group discussions and organizations.

-----  
**TABLE II ABOUT HERE**  
-----

From each of the six participating organizations, up to five representatives were involved in discussions, either in individual interviews or group meetings. All meetings were arranged via the key contact who ensured that staff with relevant knowledge regarding the organization's responses to the threat or act of terrorism were involved. In addition, in each organization the CEO or MD was interviewed where practical, as were the operational level managers such as those who managed security in the specific operations such as venues and airports, as well as those involved in managing external public relations, research and personnel. All informants were involved in strategic and operational level decisions regarding the organization's safety and security. By including both the strategic and operational level managers in the sample, the data represented a wide overview of threat within each organization.

Once data had been collected and interviews transcribed, the authors looked for patterns, themes and the overall stories revealed in the data. Following Pentland (1999) and Langley (1999), we

examined the transcripts for focal actors, voices, actions, choices, and events that were woven into an empirically based story about how and why something happened. In this way, we could construct a number of stories about and attitudes toward perceived threats from terrorism. This was carried out manually with each of the two authors independently identifying themes. This coding procedure revealed three major themes in perception and four major themes of action, each of which both authors had independently identified. Like Ball and Wilson's (2000) study of computer based monitoring, we use these themes as the basis for discussion in this paper. The three themes of perception are 'threats can be measured and prioritized', 'regulation will take care of the threat', and 'threat from terrorism is a top priority'. The four major themes of action are 'work with other organizations in the supply chain', 'rely on other organizations', 'rely on regulation and information', and 'business as usual comes first'.

As Pentland (1999) and Langley (1999) point out, stories and description are one thing, validity is another. In order to ensure validity, we involved all six organizations in feedback sessions. These took the form of the authors organizing two events in London to which representatives from all six organizations were invited. It proved impossible to get dates to visit each organization separately, so a joint event seemed a workable alternative. The events were workshops focused on the 'visitor economy' and the results from the current paper were disseminated. Each organization had at least two representatives at the workshops. In neither workshop were factual changes to the stories and descriptions requested. Our interpretations were viewed as well-crafted and have formed the basis for internal discussions in each of the six organizations. A follow-up study is planned to ascertain what changes (if any) have resulted from more current terrorist attacks (such as 7/7 in London) and from our feedback.

## **ANALYSIS**

### **Threat can be Measured and Prioritized**

Without exception, managers assumed threat was measurable and assessable through the probabilities of normal distribution, rather than being viewed as an immeasurable uncertainty. Managers assess the threat of terrorism in terms of the amount, severity and nature of losses which might occur and this allows them to assign priority (or not) to the threat. For example, managers in the Convention Centre perceived many other threats to be of a greater threat to them than terrorism. Such priorities were calculated on the basis of prediction of what would normally



happen (Cerulo 2007). Priorities revolved around the content and type of work commissioned and presented.

*“risks” are associated with being controversial - with the type of work profiled - the riskier it becomes depends on how the patrons will interpret it’ (Programme Manager).*

*‘Programming is high risk. I mean you can still find an audience for it, you still might have a sold out house for something that’s very extreme, - but as an arts organization your remit is to broaden the art form, not just keep with the status quo’ (Events Manager).*

They also perceived other threats to be important, singling out the latest foot and mouth epidemic in the UK as an example. Risk was primarily perceived as the flow of tourists into the country and region and the related fall in demand for conferences and events.

*‘... if you think about the effect of foot and mouth or some sort of other big disaster - there’s more risk than just terrorism. Obviously a terrorist threat has an impact, but to a certain extent you do what you can do and then you just have to get on with it’ (General Manager).*

*‘Foot and mouth wasn’t that long ago, it destroyed tourism and nearly all this business. This has a bigger effect on conference volumes than terrorism’ (Sales and Marketing Manager).*

The Arts and Entertainment Centre informants also did not ascribe priority to threat from terrorism using an analysis which relied squarely on what had happened in the past, using black humour to paint the retrospective picture (Weick 1995).

*‘The IRA had a bomb go off here many years ago, which was almost a joke. I think he blew himself up by mistake. It’s one of these stories that become part of the mythology of the place “oh yes well the IRA tried to blow it up but that wasn’t very successful and they were obviously in the wrong place anyway, they were trying to find the Parliament and found themselves on the wrong side of the River”’ (CEO).*

The ‘organizational memory’ (Weick 1995) had already been formed by this semi-humorous event. Even recent terrorist actions, such as 9/11, were perceived as being scalable in nature. The centre of business simply shifted location.

*‘There is no question re the balance between New York and London, - the cultural centre of the world has shifted perceptively since 9/11 to London. New York is like the rest of America, it appears to be suffering substantially from the idea that it is not an easy place to go any more’ (Marketing Manager).*

For the Tour Operator, the perception of threats from terrorism revolved around the impact it had on destination choice by customers.

*‘People are saying - I’m safest anywhere - it doesn’t matter where I go, because it can actually happen anywhere, and it’ll never happen to me, - so people are willing to travel, and*

*that's the reason that people still travel even though there is this huge terrorist potential to hit somewhere' (Sales Manager).*

## **Regulation Will Take Care of the Threat**

The three organizations in the aviation sector rely on regulation as both a signalling device (of potential dangers from terrorism) and as a form of industry standard.

*'It's the airline's own regulatory and compliance authorities who have got to become much tighter, and that's a big issue for a lot of the airlines because they're not set up for it; they're set up to speed up turnaround but they're not set up so well. That is a big issue at the moment for the Department of Transport, everybody looking at how do you manage the turnaround to both be streamlined, but also totally secure' (Security Manager).*

Of the regulators, the Civil Aviation Authority (CAA) figures large in the sector as standard setters.

*'The CAA will not allow British aircraft to fly into airports that don't have the appropriate regulations in place. Which is why, for example, British Airways does not fly into Baghdad at all; one of the reasons is because Baghdad International Airport does not have IKO standard. We are not talking about the risk of scud missiles but the airport itself in terms of how security is handled at the airport. It has to meet certain guidelines in terms of the sort of national guidelines and probably federal aviation, some federal aviation authority guidelines. It doesn't currently meet IKO standards' (CEO, Airport).*

Externally imposed regulations were often interpreted to emphasize their economic consequences rather than focus on threats from terrorism. Regulations were argued to constrain the airline, because they threatened their low-cost niche in the industry. They could be regulated out of business.

*'There's a temptation with EU control and EU law, expanding its influence more and more, that they start to over-regulate potentially the consumer situation or over-regulate the industry and actually eliminate consumer choice rather than increasing it as we go forward. All that leads to is just everybody having to converge what they're offering in terms of a product. So you start to eliminate consumer choice, whereas at the moment somebody pays peanuts and they don't expect to get with that an insurance policy of knowing they'll be put up in a hotel or a free meal and the choice is theirs' (Regulatory Affairs Manager).*

## **Threat from Terrorism is a Top Priority to Managers**

Perhaps not surprisingly, managers in the aviation sector ascribe priority to perceiving greater threat from terrorism than from regulation, because their perceptions are of events which can have devastating effects on their business (as well as their passengers). For example, organizations supplying food to airlines recognize that introducing poison or a bomb on board an aeroplane via the supplied cabin food is more likely to happen in terms of probability than a terrorist getting on board as a passenger. It is simpler to infiltrate the food preparation areas than the aeroplane itself.

A common theme overall, however, is that managers in all six organizations perceive threat based largely on probabilities and normal distributions (both of occurrence and of how devastating to the business any outcome would be). The amount and severity of likely losses shape and focus managers' perceptions of threat, much along the lines of a standard model of financial risk (Hertz and Thomas 1983). Such a perspective, of course, falls squarely under the resilience paradigm, assuming both a high degree of managerial agency and of the ability of managers to plot and predict risks along different forms of probability distributions.

## **Threat Management in Action**

### **Work With Others in the Supply Chain**

Organizations which supply the aviation sector consumables such as catering have traditionally adhered to strict quality standards and threat audit processes to try to ensure consistent standards in product delivery both domestically and internationally. Standard risk management practices already exist:

---

*'Our reputation relies upon not poisoning passengers. So the whole training, the compliance regulation, all the controls we put in to ensure total food hygiene and sort of batch traceability goes all the way through our business, because we are in a very high risk catering environment with the airlines' (Director of Catering Operations).*

---

Suppliers work closely with their clients to ensure that their threat management processes are robust. Some client organizations have traditionally taken the initiative and insisted their suppliers comply with standards set by themselves:

*'I think BA was in the vanguard of this because the security requirements on us as a caterer were hugely ahead of what the industry standards were, industry standards regulated by the Department for Transport' (Quality Assurance Manager).*

Airlines in particular, have historically worked with their suppliers to develop initiatives to ensure that the security of the supplier and, therefore, the airline is secured:

*'Back in 1999, when we signed a contract with BA, we had BA security work with us through a whole programme. We made big investments in exterior perimetering of each site, then you actually have positive access into the building for all suppliers, staff and contractors coming in. To ensure we have a completely secure environment, there has to be positive access to get in to one of our kitchens. Everybody has to wear name badge, we give £25 to any of our staff who challenges anybody who is in there without proper badging, to create a sealed environment' (Security Manager).*

Airlines such as British Airways not only secure the site, but due to the variety of different items which need to be loaded onto each 747 leaving Heathrow, for example, also ensure that final checks are conducted. Informants also commented on the increased emphasis on security management since September 11<sup>th</sup> (9/11). The impact of international terrorism meant that suppliers to the aviation sector had to further tighten their threat management processes in order to respond to increased security concerns, including the fear of further terrorist attacks:

*'What has come very much to the fore since September 11<sup>th</sup> is the whole airport security, so the whole issue of getting a bomb onboard an aircraft; it has always been seen that catering would be the easiest area for a bomber to actually get a bomb onboard an aircraft' (Security Manager).*

*'Some of the airlines actually have their own staff in our kitchen doing security during the day, especially the American airlines' (Quality Supervisor).*

Department of Transport representatives visited unannounced to gain access to the kitchens, to try to find loopholes:

*'In two years, we've had two incidents out of probably 50 or 60 where they've actually got access to them, but they've never got through into the production area' (Security Manager).*

Informants distinguished between the levels of threat associated with servicing long-haul charter and scheduled airlines from those associated with the low-cost carriers.

*'The low cost carriers are the simplest, because there's no service on board, once we load in the morning, it's loaded for the day. We often top up with sandwiches and water, but that just*

*involves one person. They don't have cabin cleaning, because their staff do all the cleaning. They chuck out the rubbish; they don't have rubbish contractors. They have optimised the model to avoid people coming on at a cost, hence they can facilitate this rapid turnaround philosophy. The simplicity of their economic model also works from a security point of view' (Catering Load Manager).*

An international code relating to airport security practices was regulated by the International Civil Aviation Authority Security (IKO). This body was charged with issuing guidelines and regulations that each national Civil Aviation Authority would enforce. Every airport has to be inspected by IKO every two years and airlines will not fly to them unless they are audited. Informants explained the national CAA's role in determining which airports national airlines were allowed to operate. Nevertheless, security professionals in the industry recognized that even this degree of investment, will never render security 'foolproof':

*'Here in the UK, Heathrow Airport has had numerous incidents of robberies and the press attempts to infiltrate security successfully, which they've done successfully. So there's no such thing as perfect security, but one of the things which an airline like British Airways (BA) would do is to layer the security so there's lots of measures which are being used along the way before you actually get on the aircraft up until the point even before the aircraft takes off. These kind of layering of security suggests that they have a reasonable angle on how to manage security within the kind of British domestic environment but the difficulty is when you go abroad' (GM Operations).*

*'Layering means customer profiling and use of CCTV in and around the airport. For example, the way people respond to the questions "did you pack your own bag?" is useful in risk reduction? It is not so much the answer people give, but their body language. This singles them out as being deserving of extra attention, so that as you then pass through all the other parts of the security chain towards actually boarding the aircraft, there are a number of opportunities to identify people as being suspicious' (MD Airport).*

BA was considered in the UK to be at the cutting edge in this area, because it had always demanded that adequate measures were in place in any airport it flew into. This high standard was seen as a common characteristic of other major flag carriers.

### **Rely on Other Organizations to Reduce Threat**

Airlines operating from the international airport in our sample included both low-cost carriers and scheduled airlines. Low-cost airlines have seemingly invested the minimum resources into security management, relying entirely upon airport infrastructure and processes to ensure that security is managed appropriately.

*'We have done extensive work after September 11<sup>th</sup> with Airtours and Thomson Airtours. It became apparent that they had no infrastructure at all, in terms of security. The margins*

*that they run are so slender that anything above and beyond the most basic getting bums on seats and getting loads of people out to holidays and turning them round again, was just beyond anything which they could even comprehend because they would just lose money' (Airport Security General Manager).*

Informants felt that this raised some questions about other low-cost carriers. Although this was one of the most regulated sectors in terms of security, airport management expected a baseline standard, the regulatory standard would be followed, which would in turn force airlines to conform. However, there were concerns about 'grey areas' which centred around situations when assessable threats became uncertainties:

*'I think the grey area comes around the sort of charter, as I mentioned charter companies who conform to the letter of the regulation on the aircraft, but it's all the other stuff around it that they perhaps don't quite meet the standards on. You can't imagine the likes of EasyJet running sophisticated passenger profiling, for example' (Security GM).*

Managers in the airline company were concerned with minimizing disruption for the customer in their risk management practices.

*'You take the example of security, there are processes devised which we tourists have to jump through these various hoops, which we actually now totally accept and actually we like, but we need to make sure that they are as customer focused as they are security focused, so we try and match process requirement with customer requirement. There are points where you'd have to say well we need to do this for the sake of security, and public will tolerate that, but there's ways it can be done. For example, a silly thing, immigration processes at the airport, I find that they're the darkest, dreariest po-faced approach, and they absolutely have a fantastic job to do, but there is no harm in a good morning. They can be just as efficient and just as ruthless. You know they're the first point of contact for people arriving in this country' (Marketing Manager).*

The airline carries nearly 5 million passengers annually. Due to tight margins in this low-cost business, the airline tried to reduce its airport security management costs by relying entirely on local airports to manage their security procedures rigorously. The airline also reduced its exposure to threat by not providing a full catering service in-flight, thereby reducing the likelihood of food hygiene problems or any catering related security breaches.

### **Rely on Regulation and Information**

The airline relied upon regulators to help risk management. Informants argued that regulation is essential for maintaining minimum standards of health, safety, fire precautions, and a range of related factors. Airline management were concerned, however, at how regulatory policy was

deployed internationally and the potential impact this could have on their operations. Regulatory policy is not standardized internationally:

*'A lot of the policy that's come in, particularly in the EU side, is great on paper, but actually when you look at the amount that's been enacted, or not, frankly on something like the French environment, and their whole regulatory system, it's just, absolutely rubbish. Nobody's abiding by that' (External Relations Manager).*

*'We would welcome the industry regulators to be far more educated about demand, the patterns and where demand is going when they are making regulations. It's so disconnected at the moment, you'd think they'd never even flown on an airline or taken a holiday, in terms of their level of understanding across the industry' (Business Development Manager).*

UK-based international tour operators rely upon British government travel information to particular overseas destinations to determine whether or not to continue to service particular destinations. The Home Office travel advisory service, therefore, has a significant influence on travel to specific destinations, directly affecting the viability and success of some key tour locations:

*'Caribbean Tourism has suffered at the hands of the Foreign Office travel advice. The impact of the travel advisory is I think very significant, but there has been debate about the impact on it. It was reported that on a Caribbean Island, Al-Qaeda had a cell there. The fact it was a Muslim group, with a local leader who expressed sympathy for Osama, ended in a shoot out. MI5 compiled reports, and seized on this and raised the ratings, so the cruise ships stopped visiting and snorkelling around this specific port. This really put the wind up all the other little Caribbean islands, maybe something like that can happen to us? It was going on at the time of the Bali attacks when there was so much scrutiny of travel advisories' (Marketing Manager).*

When a destination is deemed to be too risky, tour operators may cease to operate there. This poses problems, however, since risk assessments need to be conducted to determine when it is safe to return to that particular destination. Part of this assessment process requires a determination of consumer reaction:

*'It must be just over 18 months ago when there was a threat to British aircraft flying into Kenya, that they would be shot out of the sky with a missile attack. So we stopped flying, everyone stopped flying and 18 months on and we haven't got our charters back in there. It was very profitable, however, this will damage Kenya for a long time, because it's faraway, it's an unknown, people don't feel safe in the first place, and when something that happens, you can cancel it, you can kill it. It's the worst thing that could possibly happen if a aircraft was shot out of the sky. That's worse than a bomb going off in a hotel, much worse. An aircraft being shot out of the sky is the most terrifying thing, whereas if they had a bomb in the one place, people believe it'll never happen to me' (GM Operations).*

Informants explained that they relied upon official Foreign Office (FCO) advice to inform decisions. They explained that the nature of risk management involved in running a tour operation was to try to manage everything in an integrated manner:

*'We have to be aware of all the different pieces (i.e.; hotels, airlines, coaches), every bit that everybody else is doing to be able to compete with them all, because we compete with everybody. That's the challenge for us; it's the ultimate risk model. We are dealing with a high turnover, low margin type risk profile. It's not just about aircraft and putting seats on an airline, which is pretty straightforward actually in terms of risk and in terms of passengers journey management, -but we have to guarantee a combination, which means we have to pay for those beds whether they are filled or not' (Yield Manager).*

In response to specific threats regarding potential terrorist attacks on tourists in specific areas, tour operators had noticed changes in consumer behaviours. Travellers reacted to various terrorist attacks and threats in different ways. Some consumers immediately altered their leisure plans whilst others became fatalistic about being directly affected by such an attack:

*'The amazing thing about terrorism is that it used to be that if a bomb went off somewhere, then people would jump somewhere else. Last year for instance, Spain had a boom year. Since we had a war over in the East, which meant that people were reluctant to go to Cyprus or even though Tunisia, - they all piled into Spain. So that was a bumper year for them. This year the Euro is going against them, and now more people feel the war is ended, - but we still have terrorist attacks, which really can happen anywhere. Okay, admittedly no one's going to go to Iraq for their holidays for quite some time, -but they are going to Egypt in bigger numbers than ever before, which is pretty close. And as we've seen [terrorist attacks] in Madrid, you could have it in an Eastern Mediterranean country, or in the UK.*

Tour operators' informants emphasized that they were frustrated at the quality of the information provided. One of the criticisms regarding FCO travel advice was that it either tended to be too general or too focused on the backpacker tourist as opposed to the business traveller or, indeed, on companies that have operations in a particular country. Hence:

*'There are a lot of steps that have been taken within the Foreign Office to take into account the criticism which they encountered from Bali where they didn't get to say enough. Also, in the India/Pakistan stand-off (the FCO warning that everybody should leave India and Pakistan because there was going to be a major confrontation) which was taken extremely seriously. It turned out to be incorrect, although it was believed that there was specific intelligence behind that, but it turned out not to really pan out the way that it was suggested and it could have cost businesses very dearly. There is still massive anger amongst many heads of security about that sort of advice, - where they probably said too much and everyone evacuated. So now they have realised they needed to focus this stuff more towards*



*business needs rather than to make it so general that it's almost worthless' (Communications Manager).*

Managers also questioned the way 'intelligence' was converted into operational level briefings. One manager observed how British Airways and Air France were forced to cancel many planes travelling into the USA based upon American intelligence, causing considerable disruption to the airlines and their passengers:

*'We saw that it got to the point that the airlines actually started to get a bit annoyed with the Americans, well pilots certainly did with the American intelligence, because it was a question of where's this coming from and is it really a problem?' (Security Manager).*

### **Business as Usual Comes First**

In the arts and entertainment organizations maintaining business as usual (rather than prioritizing terrorism) was viewed as key, although there was some evidence of putting practices in place to counter terrorism in recent months. Typically, informants would argue that they were 'used to' high risks. For example, many venues in the UK have been geared towards managing security for high-profile visitors such as the Queen, or for high-risk performers such as Israeli dance companies. Paradoxically, since high-profile visitors were the norm, the management of risk and security was considered by many informants to be a relatively routine matter.

*'You do what you can do and then you get on with it. I mean in a way that's what we've always done. London and England's had a history of problems, people just get on with it. I think in America you get such a huge reaction the first time something like that ever happens, and then you get reactionary policies and strategies put in place' (Security Manager).*

Entertainment venue managers recognized that their centrally located centres may be the target of international terrorists wanting to make high-impact statements.

*'If you're an icon in that case, they would want to blow up it up because it actually makes a major international statement like the World Trade Centre. Some have had to invest a huge amount of money in recent times in security infrastructure... you can't drive cars in and you can't do all sorts of things now that you could have before 9/11, - who would have actually thought about them as issues before 9/11?' (Front of House Manager).*

However, implementing new practices seemed problematic since the reaction to a perceived threat largely relied on the judgement of the manager on the day:

*'Even running this place now has changed, our whole business is predicated on accessibility from 10 o'clock in the morning until 12 o'clock at night and it's very different. There are three million people who visit the buildings and the facilities just during the day and a million who buy tickets at night. The issue is how can do you make a judgement that says, you know, do I shut the building down, do I move away from what the nature of my business is on the chance that out of all the buildings in all the world, this is the one they're going to*

*come to? So you are actually looking at risks but then having to make judgements which are almost impossible to actually to determine' (Security Manager).*

As public building managers, they were seeking to learn from other incidents involving large numbers of the public in order to consider how to manage possible terrorist attacks:

*'Regarding blowing people up at the Olympics or on the Madrid train echoes one of my nightmares. Running halls with lots of people in them means that someone comes in and does something like the Moscow experience, and the damage it can cause is remarkably fast to a lot of people before anyone is able to respond' (Front of House Manager).*

Informants considered that their main challenge was the sheer volume of events held each year and determining the appropriate scale of security. It was reported that unlike the Olympics, hall managers had to ensure a constant level of security for over a thousand events a year, held inside the centre. This posed dilemmas for management regarding how to operationalize a risk management framework on this size and scale. In the end they opted for maintaining business as usual:

*'We do random bag checks. We don't allow certain things to be taken into the theatre. We've already had to substantially increase the security coverage over the last two and a half years but the idea of having to search every person coming to over 100 events; you have to make a decision. Do I keep the building open in the daytime and allow people to come into the place, or, do I actually shut the building down and only open it up for concerts, for people with tickets?' (General Manager Operations).*

Informants argued that a tight security policy would have ultimately deleterious effects on overall business performance.

*'The risk there means I can't make that viable because I've got businesses, shops, restaurants, various other things that sit within it. So there is a risk to return equation that you're continually having to juggle, which I never even remotely thought about when I started in this business and it's a huge issue now. But business must come first' (CEO).*

Table III summarizes both perceptions and actions toward the risk of terrorism in the six organizations.

---

**TABLE III ABOUT HERE**

---

## **DISCUSSION**

The data reveal seven broad themes. The most common (across all six organizations) perceived the threat of terrorism as a risk which could be assessed using probability assessments, or variations of these using other risk management techniques. These managers assumed that management actions would reduce risk by increasing organizational resilience to uncertainty, largely by increasing operational excellence. However, deeper investigation revealed that the same organizations also exhibit signs of systemic features which were termed by informants 'grey areas' of uncertainty. These fell outside concerns for operational excellence. Regulation (at airports for example) was presumed to cope with uncertainty so managers assumed they need not take action to address these risks, whilst other grey areas (such as possible customer profiling) were not implemented at all.

A further feature of the data reveals what Gilovich, Vallone and Tversky (1985) have termed the 'hot hand' fallacy (in basketball) where individuals might erroneously perceive causal regularity in random sequences of events (in the tossing of a coin, for example). Given two sequences of heads (H) and tails (T) HHHTTT and HTHTTH, individuals will assume the former sequence is significantly more likely to continue HHH than the latter, on the strength of its apparent 'pattern' when, in fact, both sequences are equally likely (Taleb 2007). As Odean (1998) has also observed, the nature of the human mind as a pattern-seeking device can easily lead to spurious causality. Examples of this in the data can be seen in the entertainment venue, where it was left to the manager of the day to use his or her judgement about the pattern of events (customers, shows, size of crowd) to assess risk. The 'assumption in use' was that previous experience - nothing had happened in the past - was an accurate guide to managing current uncertainties, with the result that managers reduce security checks and overall vigilance. These broad patterns draw upon either both how managers frame their perceptions and how they deal with uncertainties in practice (what decisions they make). These are examined in more detail below.

### ***Management Framing***

Framing refers to definitions of organizational reality which shape both understanding and action (Gioia 1986) and includes '*assumptions, knowledge and expectations ... expressed through language*' (Orlikowski and Gash, 1994: 176). Framing helps characterize how managers perceive uncertainty, which influences action.

The data reveal patterns and regularities in the framing of perceptions. Such a stance is consistent with Giddens' (1984) notion of 'bracketing' whereby some aspects of organization such as security

threats or terrorism are perceived to be unproblematic and, hence, are not given priority. They are taken-for-granted patterns in the social structure of organization (Orlikowski 2000) which emerge as managers make sense of their context. Structure and agency are thus intertwined (Reed 1997).

Not all uncertainties concern acts of terrorism, or in trying to predict where terrorists may strike next (Mayntz 2004). Economic and operating uncertainties also have to be dealt with and decisions made on how to deal with these risks. For example, low-cost airlines allocate very few resources to anything other than making a margin on minimum outlay to get a plane full of passengers in the sky. Since managers in the airline recognize the importance of terrorism, this is at first sight an unusual finding. However, the data indicate that this is a function of assumptions and expectations. Managers framed their responses both in terms of *assuming* airport authorities would do the job of customer profiling and security, as well as *expecting* such processes to take place for every flight. Such framing resonates with Cerulo's (2007) arguments of positive asymmetry and assumptions of the normality of distribution and occurrence of events. Airport authorities were assumed always to carry out such activities, leaving the low-cost airline to concentrate on operational excellence.

Managers in the arts and entertainment centre assumed that high-risk (cutting-edge) programmes were more of a threat than security. As a result, they had cut down security checks in the centre and encouraged greater volumes of customers. The use of humour (portraying an earlier IRA threat as inept) underscores this framing (Goffman 1974) and corresponds to Gioia's (1986) notion of *stories* which become institutionalized and which influence what actions managers deem to be appropriate. This also resonates with Taleb's (2007) description of inaccurate perceptions concerning organizational histories by managers.

Tour operators argue that people travel without fear since they do not expect any attack to happen to them. Tour operator managers also thought this way, and sold their packages to customers on the basis that – OK, there is a huge potential for a terrorist strike almost anywhere in the world – but that it was not going to happen on this tour. Both customers and managers engage in what Bougon et al. (1977) and Eden et al. (1992) term shared cognitive mental maps and engage in 'false' assumptions of normal distributions (Cerulo 2007). Both parties create a series of expectations to reduce the apparent/expected threats being faced. These expectations hinge around alternative destination choices in the event of a bomb going off (in Madrid, for example). Customer and tour operator then construct a frame of reference that 'assures' passengers that an alternative destination is safe.

### *Management Practices*

In all six organizations, managers were aware that a tight security policy could have a deleterious effect on overall business performance. There was a trade-off between implementing security and making profits. In our sample, the economics of business largely took priority over managing security. This was most manifest in either relying on other organizations in the supply chain (for example, low-cost airlines assuming airports would conduct all security checks) or in arguing that other risks were more important (getting customers through the door was the top priority as in the entertainment venues).

Low-cost airlines allocate very few resources to anything other than making a margin on minimum outlay to get a plane full of passengers in the sky. As one informant from the airport operation noted: *'low cost airlines spend as little as 50p per passenger with regard to their security'*. This finding resonates with Tarlow and Santana's (2002) data, which show the limits of risk perception in security professionals and how easily they can be influenced by context. In some situations, security professionals will deny any problem exists, or argue that someone else will handle it (Tarlow and Santana 2002: 424).

In cases 5 and 6, drama performances are prioritized over security measures in the implementation of decisions. The argument from informants is that the nature of the performance put on by entertainment centres strongly influences the numbers of patrons. Too many avant-garde or unpopular commissions can spell financial disaster for these organizations. This was described as the most important risk facing these organizations, even though threats from terrorism were acknowledged to be high for these public arenas. A combination of a previously bungled terrorist attack and the assumption that it won't happen here (because when security was relaxed, nothing happened) resonates with the arguments of Gilovich, Vallone and Tversky (1985), Odean (1998) and Cerulo (2007), where assumed patterns and probabilities, accumulated in the past, influence current actions.

## Conclusions

Framing and practice seem intertwined. Individuals' perception of their context influences the actions they take and avoid (Cerulo 2007). Because managers perceive the threat from terrorism as seemingly calculable and largely corresponding to a normal distribution of probability, they apparently cluster around the same frameworks for analysis and action, for example assuming measurement is possible and that regulation will act as a kind of insurance (Cerulo 2007: 15). The data indicate that managers appear to employ methods and assessment tools that treat virtually all risks as economic in character. This form of 'traditional' risk analysis has been prevalent in the management literature for at least four decades (see, for example, Fiegenbaum and Thomas (1988), Hespos and Strassmann (1965)).

This reveals a gap in the ability of existing management tools and methodologies to deal with current threats facing the six organizations in our sample. Highly uncertain terrorist threats, management practice needs to develop different risk assessment techniques and practices that are not solely derived from a predictable perspective based on normal distributions and probabilities. This is because belief in data which follows a regular pattern (such as the average height of human beings, or the non-occurrence of a terrorist attack) is an ingrained part of human cognition. As Cerulo (2007: 34) argues, observation of a hundred humans would reveal a good picture of average height and even if there were one surprise (large or tall) it would not be consequential on the average and, hence, on how average height was reported. In a similar vein, the extreme irregularity of terrorist attacks appears to have little influence on the way managers view and implement strategies to cope with these extreme uncertainties. Framing and action therefore both appear conservative, as they are revealed in the current data. Put another way, consequential events and improbability are weighed and balanced significantly in the favour of improbability.

Knowledge and information appear to play an important role in both framing and action. The data indicate that levels of risk increase as information becomes either scarce or incomplete. This concurs with March's (1999) emphasis on the role of intelligence in effective decision making. All organizations in our sample relied upon information supplied to them by government agencies. Such intelligence was valuable, but usually out of date or incomplete. Decisions are nearly always made in the context of incomplete or ambiguous information. Empirically, Hickson et al. (2003) and Miller et al. (2004) demonstrate the key role of accurate and complete information in helping secure effective implementation. It is arguable that the greater the ambiguity and the

incompleteness of information for decision makers dealing with threat, the greater is the exposure to (and degrees of) risk. Turner (1976) found this phenomenon also applied to ineffective disaster management. Managers in the current study nearly always tried to make incomplete information 'complete'. For example, the tour operator managers had two strategies toward incomplete information. They either tried to fit information into their business model, ignoring what did not fit (they legitimized this behaviour arguing that information had proven inaccurate in the past); or they began to frame their own interpretations of incomplete data. For example, warnings from the Foreign Office not to travel to certain destinations (such as Egypt) were largely ignored on the basis that two strikes in quick succession were extremely unlikely.

Although the sample organizations are in the same broad industry sector, there was little evidence of learning, or transfer of knowledge, between organizations in the sector (Legge et al. 2007). The transferred experience of one organization (or a group) in the face of such threats and outcomes could be the basis for greater inter-organizational learning. Even natural exogenous events (such as the Asian tsunami in December 2004) have the capacity to be the basis for a significant amount of organizational learning (e.g. scalability, prediction, evacuation etc) (Cerulo 2007).

It seems difficult to regulate for threat except at the most basic (predictable) level. Regulation means, for example, that organizations have to build high and robust walls around a nuclear power station, to satisfy the letter of regulation. However, managers do not know if terrorists are likely to crash an aeroplane, release poison gas or do something as yet unforeseeable. Thus, changes may need to be made to the ways in which managers perceive risk (Cerulo 2007). People in organizations may need to think about risks in different ways and, certainly, they need to be skilled in gathering information which they can comprehend, which they can interpret as being useful to analysing and assessing risks which do not conform to the prevailing notion of the normal distribution.

In this paper we have taken two constructs (framing and action), since our data were able to speak to these themes. There are, of course, many more frames, such as stories, folklore, rituals and metaphors which could form the basis of more detailed studies of rare events and how individuals interpret and react to them. For example, airlines, tour operators and, by extension, other types of organizations are exposed to a hybrid form of risk which includes contagious diseases, terrorism, the economic risks of market exposure and the risks associated with incomplete or insufficient information. (Beck 1992 and 2000; Luhmann 1993; Perrow 1984; Turner 1978). For all its

limitations, this paper has tried to depict how managers perceive and act upon one of these rare events – the threat of terrorism. A key overall finding is that none of the six sample organizations could be described as high reliability organizations in the sense outlined by Weick and Sutcliffe (2001). This is primarily because managers try to scale the unscalable (applying techniques of prediction and planning to unpredictable events) whilst at the same time relying on a range of institutionalized factors (such as what happened in the past driving current actions, or relying on other organizations to address risks faced by the focal organization) to inform and justify their actions in the face of high uncertainty. This combination of the ‘ludic fallacy’ and institutionalized factors could, ultimately, be an even more dangerous phenomenon to organizations than the threat of terrorism itself.



## REFERENCES

- Ball, K., and D. C. Wilson (2000) 'Power, control and computer-based monitoring: repertoires, resistance and subjectivities'. *Organization Studies* 21/3: 539-566.
- Beck, Ulrich (1992) *Risk society: towards a new modernity*. London: Sage.
- Beck, Ulrich (2000) *Power in the global age*. London: Polity Press.
- Bentley, Tim, and Stephen J. Page (2001) 'Scoping the extent of adventure tourism accidents'. *Annals of Tourism Research* 28/3: 705-725.
- Bhide, A. and Stevenson, H. (1992). 'Trust, uncertainty, and profits'. *Journal of Socio-Economics*, 21, 91-208.
- Bougon, Michel, Karl Wieck, and Din Binkhorst (1977) 'Cognition in organizations: an analysis of the Utrecht Jazz Orchestra'. *Administrative Science Quarterly* 22/4: 606-639.
- Bryan, L. L., and C. Joyce (2005) 'The 21<sup>st</sup> century organization'. *McKinsey Quarterly* 3: 1-6.
- Callander, Marie, and Stephen J. Page (2003) 'Managing risk in adventure tourism operations in New Zealand'. *Tourism Management* 14: 13-23.
- Cerulo, Karen A. (2006) *Never saw it coming: cultural challenges to envisioning the worst*. Chicago: University of Chicago Press.
- Cornish, P., (2007) *Britain and Security*. London: The Smith Institute.
- Czinkota, Michael, Gary A. Knight, and Peter W. Liesch (2004) 'Terrorism and international business: conceptual foundations' in *Terrorism and the international business environment: the security-business nexus*. G. Suder (ed.). Cheltenham: Edward Elgar.
- Czinkota, Michael R., Gary A. Knight, Peter W. Liesch, and John Steen (2005) 'Positioning terrorism in management and marketing: research propositions'. *Journal of International Management* 11: 581-604.
- DiMaggio, P. J., and W. W. Powell (1983) 'The iron cage revisited: institutional isomorphism and collective rationality in organizational fields'. *American Sociological Review* 48/2: 147-160.
- Eden, Colin, Fran Ackermann, and Steve Cropper (1992) 'The analysis of cause maps'. *Journal of Management Studies*. May, 29/3: 309-325.
- Eisenhardt, Kathleen M. (1989) 'Building theories from case study research'. *The Academy of Management Review* Oct 1989 14/4: 532-551.
- Faulkner, B. (2001) 'Towards a framework for tourism disaster management'. *Tourism Management* 22/1: 135-147.
- Fiedler, F. E. and Garcia, J.E. (1987). 'New Approaches to Leadership, Cognitive Resources and Organizational Performance'. New York: Wiley.

- Furnham, A. (1992). *Personality at Work*. Lexington, MA: Lexington Books.
- Gephart, Robert P. Jr. (1984) 'Making sense of organizational succession: an ethnomethodological approach'. *Administrative Science Quarterly* 28: 553-581.
- Gephart, Robert P. Jr. (1988) 'Managing the meaning of a sour gas well blowout: the public culture of organizational disaster'. *Industrial and Environmental Crisis Quarterly* 2: 17-32.
- Gephart, Robert P. Jr. (2004) 'Normal risk'. *Organization and Environment* 17/1: 20-26.
- Gephart, Robert P. Jr., and R. Pitter (1993) 'The organizational basis of industrial accidents in Canada'. *Journal of Management Inquiry* 2/3: 238-252.
- Giddens, Anthony (1998) *The politics of risk society*. Cambridge: Polity Press.
- Gilovich, T., R. Vallone, and A. Tversky (1985) 'The hot hand in basketball: on the misperception of random sequences'. *Cognitive Psychology* 17, 295-314.
- Gioia, D., Henry P, and Jr, Sims (1986) 'Cognition-behaviour connections: attribution and verbal behaviour in leader-subordinate interactions'. *Organizational Behaviour and Human Decision Processes* New York. 37, April: 197-230.
- Glaser, Barney G., and Anselm L. Strauss (1967) *The Discovery of Grounded Theory: Strategies for Qualitative Research*. Chicago: Aldine Publishing Company.
- Goffman, Erving (1974) *Frame analysis: an essay on the organization of experience*. Cambridge, Mass: Harvard University Press.
- Greenaway, Rob (1996) 'Thrilling not killing: managing the risk tourism business'. *Management* May: 46-49.
- Greenwood, R., and C. R. Hinings (1988) 'Organizational design types, tracks and the dynamics of strategic change'. *Organization Studies* 9/3: 293-316.
- Gummesson, Evert (1991) *Qualitative methods in management research*. London: Sage.
- Hamel, Gary, and Liisa Valikangas (2003) 'The quest for resilience'. *Harvard Business Review* September: 52-63.
- Hedberg, B. (1981) 'How organizations learn and unlearn', in *Handbook of Organizational Design* Vol. 1. P. C. Nystrom and W. H. Starbuck (eds). New York: Oxford University Press.
- Hertz, David, and Howard Thomas (1983) *Risk analysis and its applications*. New York: Wiley.
- Hespos, Richard. F., and Paul A. Strassmann (1965) 'Stochastic decision trees for the analysis of investment decisions'. *Management Science* 11/10: 244-259.
- Hickson, David J., Susan Miller, and David C. Wilson (2003) 'Planned or prioritized? Two options in managing the implementation of strategic decisions'. *Journal of Management Studies* 40/7: 1803-1836.
- Keynes, J. M. (1921) *Treatise on probability*. London: Macmillan.

- Knight, Frank H. (1921) *Risk, uncertainty and profit*. Chicago: University of Chicago Press.
- Langley, A. (1999) 'Strategies for theorizing from process data'. *Academy of Management Review* 24/4: 691-710.
- Laqueur, Walter (1999) *The new terrorism: fanaticism and the arms of mass destruction*. London: Phoenix Press.
- Legge, K., B. Sullivan-Taylor, and D. C. Wilson (2007) 'Management learning and the MBA: the beast that morphed into a chameleon'. *Management Learning* 38/4: 440-457.
- Luhmann, Niklas (1993) *Risk: a sociological theory*. Berlin: Aldine de Gruyter.
- March, J. G. (1981) 'Footnotes to organizational change'. *Administrative Science Quarterly* 26: 563-577.
- March, J. G., and J. P. Olsen (1984) 'The new institutionalism: organizational factors in political life'. *The American Political Science Review* 78/3, Sept: 734-749.
- March, James G., editor (1999) *The pursuit of organizational intelligence*. Oxford: Blackwell.
- Mayntz, Renate (2004) 'Organizational forms of terrorism hierarchy, network, or a type of sui generis?' MpifG Discussion Paper. Germany: Max Planck Institute for Societies.
- Meyer, Alan D. (1982) 'Adapting to environmental jolts'. *Administrative Science Quarterly* 27: 515-537.
- Meyer, A. D., V. Gaba, and K. A. Colwell (2005) 'Organizing far from equilibrium: nonlinear change in organizational fields', *Organization Science* 16/5: 456-473.
- Miller, Susan, David C. Wilson and David J. Hickson (2004) 'Beyond planning: strategies for successfully implementing strategic decisions'. *Long Range Planning* 37: 201-218.
- Odean, T. (1998) 'Are investors reluctant to realize their losses?'. *Journal of Finance American Finance Association* 53/5:1775-1798.
- Oliver, C. (1991) 'Strategic responses to institutional processes'. *Academy of Management Review* 16: 145-179.
- Omand, D. (2006) 'In the national interest: organising government for national security'. *The DEMOS Annual Security Lecture*. London: Demos.
- Orlikowski, Wanda, and Debra Gash (2000) 'Using technology and constituting structures: a practice lens for studying technology in organizations'. *Organization Science* 11/4: 404-428.
- Paraskevas, A. and B. Arendell (2007). A Strategic Framework for Terrorism Prevention and Mitigation in Tourism Destinations. *Tourism Management*, 28/6: 1560-1573.

- Pentland, B. T. (1999) 'Building process theory with narrative: from description to explanation'. *Academy of Management Review* 24/4: 711-724.
- Perrow, Charles (1984) *Normal accidents: living with high risk technologies*. New York: Basic Books.
- Perrow, Charles (1999) *Normal accidents: living with high risk technologies*. Princeton: Princeton University Press.
- Powell, W. W. and P. J. DiMaggio (1991) *The new institutionalism in organizational analysis*. Chicago, University of Chicago Press.
- Reed, Mike (1997) 'In praise of duality and dualism: re-thinking agency and structure in organizational studies,' *Organization Studies*. 18/1: 21-42.
- Roberts, Karlen. (1990) 'Some characteristics of one type of high reliability organization'. *Organization Science* 1: 160-176.
- Scott, W. R. (1987) 'The adolescence of institutional theory'. *Administrative Science Quarterly* 32/4: 493 -515.
- Scott, W. R. (1995) *Institutions and organizations*. Thousand Oaks, CA: Sage.
- Starbuck, W., and M. Farjoun, editors (2005) *Organization at the limit: NASA and the Columbia disaster*. Oxford: Blackwell.
- Sullivan-Taylor, B. and D. C. Wilson (2007) 'Resilience and complacency in the private sector' in *Britain and Security*. P. Cornish (Ed.). London: The Smith Institute.
- Taleb, Nassim (2007) *The Black Swan: The Impact of the Highly Improbable*. New York: Random House.
- Tarlow, Peter E., and Gui. Santana (2002) 'Providing safety for tourists: a study of a selected sample of tourist destinations in the United States and Brazil'. *Journal of Travel Research* 40/4: 424-431.
- Thompson, James D. (1967) *Organizations in Action*. New York: McGraw-Hill.
- Turner, Barry (1976) 'The organizational and interorganizational development of disasters'. *Administrative Science Quarterly* 21/3: 378-397.
- Turner, Barry (1978) *Man-Made Disasters*. London: Wykeham.
- Van Maanen, John (1983) *Qualitative Methodology*. Beverly Hills: Sage.
- Vaughan, Diane (1990) 'Autonomy, interdependence and social control: NASA and the space shuttle Challenger'. *Administrative Science Quarterly* 35: 225-257.

Vaughan, D. (2005) 'On slippery slopes, repeating negative patterns and learning from mistake' in *Organization at the limit: NASA and the Columbia disaster*. W. Starbuck, and M. Farjoun (eds). Oxford: Blackwell.

Weick, Karl (1979) *The social psychology of organizing* (2<sup>nd</sup> Edition). Reading MA: Addison-Wesley.

Weick, Karl (1995) *Sensemaking in organizations*. London: Sage.

Weick, Karl E., and Kathleen M. Sutcliffe (2001) *Managing the unexpected - assuring high performance in an age of complexity*. San Francisco, CA: Jossey-Bass.

Wensley, R. (2003) 'Strategy as intention and anticipation' in *Images of Strategy*. S. Cummings, and D. C. Wilson (eds). Oxford: Blackwell.

**TABLE I: THE SAMPLE ORGANIZATIONS**

<b>Company</b>	<b>Type</b>	<b>Description</b>	<b>Scale of Operations</b>
1	Supplier to the aviation sector	One of the largest UK suppliers of retailing and catering services for airports and airlines	200 outlets in 15 countries and 83 airports across five continents
2	Low-cost airline	Based at a regional UK airport offering no-frills airline and related travel services	9.4 million passengers/year
3	International tour operator	A market leader in the UK inclusive holiday market, operating resorts and travel agencies, servicing over 40 holiday destinations	33 million passengers/year
4	International airport	One of the UK's fastest growing regional airports with in excess of six million passengers travelling on domestic and international flights.	3,500 travel agencies; 79 tour operators in 18 countries; over 120 aircraft; 37 incoming agencies in 31 countries; 12 hotel brands in 28 countries with 285 hotels and around 163,000 beds; 10 cruise liners
5	International convention centre	One of Europe's largest multi-arts and conference venues, providing art, music, film and theatre	Europe's largest centre for the arts. Concert and dance venue, seven shops and catering units
6	International arts and entertainment centre	An integrated entertainment complex providing concerts, dance, performances, films, literature, education, and the visual arts	One of the UK's largest centres comprising multiple stages, arenas and screens

**Table II: Key Informants**

<b>Sample Organization</b>	<b>No. of Informants</b>	<b>Role of Interviewee</b>
Catering supplier	5	Chief Executive MD Retail & Catering, UK & Ireland Group Communications Executive Operations Director, Heathrow Airport Operations Manager (Group discussions in addition)
Airport	5	Managing Director (#1) Managing Director (#2) Airport Sales and Marketing Manager Operations Director Security Manager (Group discussions in addition)
Airline	4	Director of Business Development Head of Sales and Marketing Europe Airport Base Manager Director of Safety and Security
Tour company	5	UK Managing Director Head of Learning and Development Head of Public Relations Chief Operating Officer Group Customer Insight Manager HR Director (Group discussions in addition)
Convention centre	3	Head of Venue Services Personnel Director Security and Safety Manager Operations Manager
Arts and entertainment centre	3	Chief Executive Head of Visitor Services House Manager Operations Manager
<i>TOTAL</i>	25	

**TABLE III FRAMING AND MANAGING THE THREAT OF TERRORISM IN BRITISH TRAVEL AND LEISURE ORGANIZATIONS**

<b>Organization</b>	<b>Perception of Threat</b>	<b>Action Repertoire</b>
<i>Catering supplier</i>	Threat can be measured Threat from terrorism is a top priority	Work with other organizations in the supply chain
<i>Airport</i>	Threat can be measured Threat from terrorism is a top priority	Work with other organizations in the supply chain
<i>Airline</i>	Threat can be measured Operational threats take precedence	Rely on other organizations to provide security infrastructure
<i>Tour company</i>	Threat can be measured Regulation mitigates threat	Rely on regulation and information before acting
<i>Convention centre</i>	Threat can be measured Operational threats take precedence	Business as usual takes precedence
<i>Arts and entertainment centre</i>	Threat can be measured Operational risks take precedence	Business as usual takes precedence



**Appendix A: Examples of Questions and Prompts in Interviews and Group Discussions**

<b><i>INTERVIEWS</i></b>	What do you consider are the biggest risks facing your organization?
	How does the threat of terrorism differ from other risk and uncertainties your organization faces?
	How do you define the threat of terrorism?
	What degrees of vulnerability to terrorism does your organization face?
	How do your suppliers/partners view the threat of terrorism?
	To what extent are individuals blind to threats from terrorism?
	To what extent are there barriers in your organization which might impede communication about possible threats?
	How does your organization operate generally to risks and crisis?
	Is terrorist related risk considered at a strategic level in the organization?
<b><i>GROUPS</i></b>	What drives/changes strategic priorities in your organization? What ensures that security matters are at the top of the strategic agenda in your organization?
	Does your organization currently have robust emergency plans in place which are known to all staff?
	How do you reassure customers and/or suppliers about your level and extent of risk management?
	How are resources allocated toward combating terrorism?  Who makes such decisions?  How would you say senior managers balance risk and control?  Since 9/11 have resources dedicated to a possible attack increased?