CHAPTER 16

Crisis management

Dolf A. Mogendorff

Research Director
Eproductive Ltd
Dorking, England

Introduction

'Events, dear boy, events'. Harold MacMillan, former British prime minister, when asked what worried him most.

While most of the time the management of hospitality operations typically takes place under relatively stable conditions, in a dynamic environment there may be periods of extreme turbulence. This may be due to internal events, such as a fire, a death or crime on the property, or external events, such as a strike by transport workers, terror incidents, extreme weather and natural disasters. This chapter will discuss how operations managers may need to respond to crises, both in the short- and longer term, for the benefit of the organization, its customers and staff and the external environment.

It would be wrong to make the bold statement that all crises can be 'managed'. Especially, external incidents which impinge on the organization can at best be ameliorated by management in its effects on that organization and its stakeholders. Even internal incidents may not be wholly manageable, simply because they might not have been expected. However, what management can do is to plan and put mechanisms in place to ensure prevention of crises where possible, the minimization of the effects of any crisis, and the recovery from those effects as quickly and efficiently as possible.

Crisis management: definition and types

Crisis management is a means of proactively preparing a company for a worst-case scenario. It involves the careful planning of approaches that will minimize the effects on its operation in both short- and longer terms. Selbst (1978), quoted in Faulkner (2001), refers to a crisis as 'any action or failure to act that interferes with an (organization's) on-going functions, the acceptable attainment of objectives, its viability or survival, or that has a detrimental personal effect as perceived by the majority of its employees, clients or constituents'. Faulkner (2001) extrapolates from this that, whilst crises tend to be induced by the actions or inactions of the organization (e.g. a fire started by a cigarette or a kitchen fire created by the non-cleaning of extractor ducting), disasters tend to be induced natural phenomena or external human action (e.g. earthquakes, tsunamis, forest fires, floods; hijackings and terrorism). Jones (2003) disputes this analysis. He agrees that Faulkner's definition of a disaster is correct, but he argues a crisis is defined as 'a crucial or decisive point or situation; a turning point'. Hence it is likely that an event (whether internally or externally caused), which could be a disaster, will lead to a crisis. Hence *by definition* it is possible to have a crisis without a disaster. He goes on to propose that disasters cannot be managed (although they might be predicted and planned for), whereas crises must be managed.

Crisis management became a catchphrase towards the end of the 1980s following incidents such as the Exxon Valdez oil spill in Alaska (seen to this day as *the* example of how not to handle a crisis), the UK's Piper Alpha, oil rig explosion in the North Sea and the Union Carbide chemical release in Bhopal in India. In each case it became clear, albeit after the events, that these crises had been preventable and could be so in the future. For instance, in the case of Piper Alpha the technology was changed to make it safer, but also to reduce sharply the number of personnel exposed to the potential hazard. In the early 1990s, management practitioners developed crisis management as a vital tool of business management to provide an orderly and efficient transition from crisis condition to normal.

Methods to deal with internal events such as breakdown of services, financial difficulties, bad publicity, loss of a key employee or manager, or strikes, fire or flooding have been developed over a number of years. External events can also create a crisis situation, for instance violent crime, drug-related crime, illegal immigration, and strikes by other employees which impact on the business (e.g. transportation or fuel workers' strikes). Even from these few examples given so far it is obvious that the operations manager has often to work not only with the rest of the management team but also with external agencies if he or she wants to be effective in minimizing the effects on operational outcomes in such circumstances.

Santana (2003) has developed an operational model of crisis management (Figure 16.1). This shows that a comprehensive effort is required at all management levels to provide an integrated approach to crisis management in terms of crisis planning, training and stakeholder involvement in designing and implementing preventive mechanisms aimed at business continuity. These matters will be discussed in this chapter.

Crisis management: planning

Crisis management planning means identifying the nature of a crisis, the steps to be taken to minimize damage and recover from the crisis, and communicating effectively throughout the

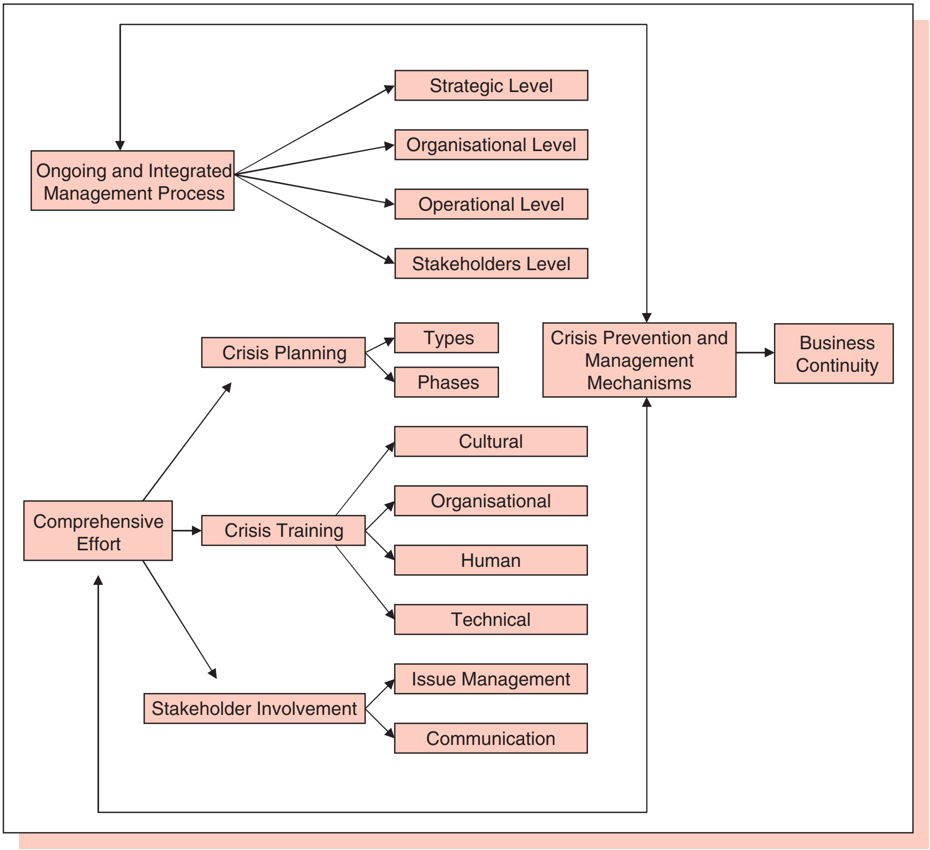

Figure 16.1
Model of crisis management (*Source*: Santana 2003).

process with all stakeholder groups to prevent harm to the company's resources, results and reputation. A relatively simple crisis created by the sudden resignation of a key staff member, such as the executive chef, could ruin a reputation built over a long period, and may require a huge effort to recover and maintain the organization's reputation. In the case that harm cannot be prevented, a plan should be in place to start rebuilding the business and the reputation as soon as possible after the event – known as crisis/disaster recovery planning. This will be discussed later in this chapter. In particular circumstances, the lack of such planning could mean the difference between the business recovering or having to file for bankruptcy.

Like any well-executed planning cycle, the crisis management process carries the added benefit of getting the management team to focus and think through the related issues. This in itself will help the team to recognize a crisis when it occurs. If a risk management process is already in place which assesses day-to-day risks, its team can be extended to deal with crisis management.

According to Campbell (2005), the team needs to comprise a core group of senior people on that site or in that business so that both policies and plans can be developed. The team will be skilled in a number of critical disciplines, assigned specific responsibilities and given the requisite authority. Team members must have an understanding both of the internal interests and of the external perspective. So, as will be seen, it requires both internal and external specialists.

A good core crisis management team needs a team leader, an incident response specialist, that is somebody who can link with the emergency services, a legal representative – and ideally both legal and financial representatives – IT, human resources, operations and recovery specialists. Last but not least is the public affairs or public relations coordinator. In addition, the core team should have access to skills banks and extra specialists who can be called on in the case of specific situations such as kidnap, ransom or special emergencies (see below). Finally the team needs a log keeper. Log keeping is a very important part of the process and in some countries a legal requirement – and such a log needs to be kept from the beginning of the planning process right through an incident and thereafter as evidence of processes planned and implemented.

The process would start by brainstorming possible crises, some of which might be specific to the property; then they should be ranked from most to least damaging in a matrix of incident types which takes account of effects on all stakeholders: customers, management, staff, suppliers, shareholders, lenders, the public at large and the media.

Incident types might include:

- altercations (amongst guests, amongst staff, between these two groups, with stakeholders and the public at large);
- various types of crime, with or without weapons, such as physical assault, sexual assault, drugs, theft, robbery, kidnap, sabotage, bomb threat or prostitution;
- personal injury whether inside the property or while in, or caused by, a company vehicle; suicide within or near the premises;
- water damage whether caused by pipe bursts or by external flooding;
- breakdown of systems with immediate safety implications, such as elevators or escalators, electronic locking systems and so on;

- fires of various types;
- medical incidents including food and other types of poisoning;
- unauthorized entry;
- property damage, internal and/or external;
- supply chain failures, especially of major and/or specialist items such as specialty foods;
- breakdown of essential systems, for example loss of power, air conditioning;
- information damage, for example to computer systems, communications systems;
- in addition, there may be crises that are not immediately obvious, such as creeping competition which, at a 'tipping point', might engender a crisis.

All such issues should be subjected to a crisis vulnerability audit – how likely is it that such a scenario might occur? A separate section might deal with (external) disaster incidents (see later in this chapter).

Then, possible damage to people, property and information for each incident type should be assessed with effects cast as widely as possible, differentiating between short- and long-term damage, identifying relevant timelines for recovery in a matrix of business functions and timescales. Both the severity and its scope should be taken into account for impact assessment. This would also clarify the interrelationships between issues, people and events, as well as the range of possible scenarios that could develop – a solution should be identified for each route. Basic questions will need to be asked, such as the following: how will customers be able to contact the business; how will suppliers supply the business; how will customers pay bills; how will the company pay suppliers? Solutions to these matters might be covered by the organization itself, by willing competitors (on a temporary basis) or by specialist business continuity suppliers who have the facilities and knowledge to provide fast and efficient support. For instance, during the SARS outbreak in Hong Kong in 2005, flight catering companies organized their shifts so that one group of workers had completely vacated the premises before the next group arrived for their shift – to minimize the possible transmission of the disease.

Once all this has been carried out, functions and individuals, both internal and external, should be identified, who could mitigate the crisis and who would be essential at such a time. These would include those who would be in charge of an emergency such as a fire, to those responsible for the safety of

ICT data and the temporary setting up of alternative facilities. With each of these individuals or teams, concrete plans should be developed and written up. Once this is done, they should be approved by authorities and regulatory agencies where relevant (e.g. fire policy).

By taking the time to think through the what-ifs, and by creating possible policies and plans, one can work more quickly should the need ever arise. It is important to be flexible; no plan should be hard and fast since one cannot plan for every scenario (who could have foreseen the exact events of 9/11?). Instead, the plans should be used as a guide to help the operation recover. Such contingency plans can also act as a guide to sanity during difficult times. In many crises, the immediate ability to respond effectively can often save lives, assets and reputations. The Hyatt Hotel in New Orleans had highly developed plans in place that enabled it to respond effectively to the 2005 flooding of that city. What was completely unexpected was that the property became the crisis management centre for the whole city, and was occupied and utilized by the various federal, state and city authorities for several months.

Training and maintenance

The plans that have been developed need to be rehearsed on a regular basis. This allows the management team to ensure that the crisis management plans are functionally up to date. People must talk in a language of response that is quick, clear and efficient and all of that must be organized beforehand. The only way to do this is to practise.

It is essential that a team member is responsible for the maintenance of relevant crisis resources that enable effective crisis management, for example immediately contactable crisis management teams (including the use of 'telephone trees'), crisis control emergency packs and so on. In a 24-h operation such as a hotel, it is vital that there is such an identified individual on duty at all times.

Plans may be rehearsed as paper-based exercises which allow clarification questions and the discussion of 'what if' written scenarios. Alternatively, the so-called telephone cascading can be done by sending out a test message without warning to everyone at the top of the telephone tree. The message then cascades down, and all persons at the bottom of the tree contact the anchor person who in turn logs those calls. In this way, the effectiveness of this communications system can be tested for speed and accuracy. The third method, and the most costly and time consuming, is the full rehearsal which provides an opportunity to test the integrity of all the parts of the plan. In a 24-h hospitality operation, this method is particularly challenging for those planning it.

The final step in the development cycle of any crisis management plan is maintenance, that is reassessing all risks and looking out for new ones, keeping the plans up to date, and keeping the teams involved and interested in this continual improvement process. The manager's aim here is to promote awareness of the need for ongoing crisis preparation and to combat so-called fire drill fatigue. Such plans, therefore, need to be tested with good and exciting simulations that challenge the team's ability to act and interact. As the crisis management process develops, one can start to tackle the more difficult scenarios. By running simulations and drills of potential crises, those who are given tasks during a crisis have the opportunity to play out their roles under stressful conditions while also being challenged intellectually. It is also important that everyone rehearses together to ensure that each individual understands their role as well as the roles of the rest of the team, building a culture of awareness.

After each such simulation, it is essential that lessons are learnt and the plans updated. A great tool is gap analysis which allows the team to model the scenario against the plan, and revise accordingly. This involves looking at the 'gap' between what should have been and what actually occurred at each step of the process and to find solutions that would close those gaps.

External agencies

Business continuity suppliers provide crisis recovery solutions to companies that are unable to continue to operate due to (unforeseen) disruption. Depending on the company, they can offer end-to-end service, from consultancy in the planning stages to the provision of all alternative ICT and other (office) services. Agreements with such organizations are known as either 'hot site' agreements with desks normally available within about 4 h of a service request or 'cold site' agreements where a temporary building can be erected on a suitable site where the company in crisis can move in about two working weeks. In each case there are issues of cost as well as the ability to rehearse such scenarios. A further option may be to make a mutual agreement with another company to use their facilities – a relatively cheap option but difficult to rehearse. Again, the function/time matrix will help decide which departments/people require such facilities, and for what time period.

There are a number of external organizations which need to be consulted and/or be kept informed and who often have expertise not available in-house. These include the local authority emergency planning officer who deals with major incidents; the emergency services (police, fire, ambulance); neighbouring businesses (managements might be able to help each other); utility companies; suppliers and (major) customers; and banks/financial services companies. Also, guests and suppliers are increasingly willing to claim their rights in an ever more litigious environment, so being able to call on the services of a good experienced legal practice is essential.

It is vital to ensure that the organization is properly insured to the right values and that, following a crisis, insurance companies can work closely with the property to help recovery as soon as possible. This requires that the insurer has all relevant information to make quick loss-adjusting decisions, such as P&L statements, occupancy and sales data, invoicing and inventory records, and reservation data so that they can project losses during the crisis.

Another key organization would be a good PR agency which has experience in the media side of crisis management. This prevents the organization's reputation being adversely affected by events and allows experts to deal with external relations while the management team is trying to get the business back on its feet. But the responsibility lies with the company to get the message right and to be seen to be involved with the crisis and its aftermath.

The following is based on key issues set out by Loretta Ucelli, a former White House Communications Director (Ucelli 2002). It sets out the key issues that senior management need to keep in mind during and after such a crisis period:

- News is global, not just local: especially where brand values have to be protected across a (geographically spread) estate, a crisis in one property might affect a whole brand;
- News is democratized (live and blogged): it travels fast and bloggers in most countries are not controlled;
- Rumours and falsehoods can spread fast, so clarity, truthfulness and timing are of essence;
- A communications protocol should be devised, so the team is clear about who the spokespersons are and to ensure that only they deal with the media;
- A communications crisis manual should be developed so that all relevant team members have clear and same instructions which they can access wherever they are and can speak with one voice;

- A stakeholder strategy should be devised so that all these parties are kept informed and up to date – the biggest problems doing lasting damage to the organization are often caused by a lack of communication with those who matter;
- Media relationships should be prioritized to those who can do most damage if they mis-report at the time of crisis and those who might be most helpful during the recovery period;
- The most senior manager possible should front the communications during and after an incident to show leadership – this requires training;
- Such a manager might need to be accompanied by an experienced PR person who can 'manage' media presentations, especially question and answer sessions;
- Respond quickly, accurately, fully and frequently.

Data protection

With organizations' ever greater reliance on data, and in particular those generated through ICT systems, crisis management needs to include clear contingency plans in case of a crisis which prevents the use of such systems or the loss of their data. Day-to-day good practice includes regular data and system back-ups, system utilities and diagnostics, secure environments (including various anti-hacking and anti-virus systems), and keeping copy data off-site in a protected environment (e.g. special safes). This may require the involvement of third parties where systems are Internet based and data held on server farms at remote sites.

In addition, there are specific matters to deal with during a crisis situation. These include:

- Keeping original software secure so that it can be uploaded again after the crisis;
- Making sure that clear responsibility has been allocated for system management, with deputizing team members to ensure constant cover;
- Mission-critical systems – those systems without which the operations manager cannot manage the basic functions of the property, for example PMS, EPOS, payroll, address lists of key personnel, customers and suppliers, will require back-up systems at all times, possibly off-site;
- Lack of an accounting system could lead quickly to cash-flow problems and loss of key management information;

- There are legal responsibilities in managing company data under Data Protection legislation, for example protecting personal information of employees; this requires staff training at all levels for normal trading conditions but is of particular importance during a crisis, for example to check on and possibly locate missing personnel;
- If the Internet is used with a reservation system, credit card details may be stored on the system, and again the organization has legal responsibilities for the confidentiality of such data;
- Crises can be created by bad system management – for example loss of data during upgrades. Careful management of such procedures is essential, including frequent back-ups and the use of master and working copies;
- Ensuring file compatibility throughout all systems makes the management of a data-related crisis much easier. Although many are now data based, there are still often compatibility issues between programmes;
- If using Internet-based systems, guarantees should be obtained from vendors on system up-time, back-up and data integrity;
- Up-to-date contact details of hardware and software support companies should be held within the crisis management system.

Information security management is now well recognized on an international basis, and quality standards organizations may offer advice under ISO/IEC 17799:2005 *Code of Practice for Information Security Management* and ISO/IEC 27001:2005 *Specification for Information Security Management.*

Effects on branding

Brands are often built over many years, but as already stated, the reputation attached to a brand can be lost in a matter of moments. Therefore, the kind of policies and procedures mentioned earlier in this chapter need to be in place to ensure the brand is protected as much as possible, and standards regained as soon as possible.

It is often the case that the brand can suffer because it is that which is in public view. A franchisor may suffer much damage to its franchise system from the fallout of a crisis in one unit – for example food poisoning. Two high-profile fires through grease built-up in ventilation systems at a major hospitality chain at a London airport and a London railway station, both of which required evacuation of these major sites, caused major travel delays and huge costs and litigation. It was the brand that suffered in the public's perception, not the unknown operator who actually caused the fires through lack of relevant training.

Another example of how a company may deal with protection of their brand relates to a fire at a large branded forest-based resort when a major fire destroyed all central facilities and services. Crisis policy dictated that staff not be laid off but to:

1. use them to deal with developing site security problems by training staff to act as security patrols;
2. use the time to retrain staff for reopening;
3. redeploy staff at other of the chain's sites.

Creative deployment of staff after this incident was done to strengthen brand standards through retraining and retaining staff loyalty through continued employment. In addition the fire created a major rethink of the design of the central facilities, with a physical division of these services in two halves intersected by a road that acts as a fire break. As will be discussed at the end of the chapter, crises can often be used as an opportunity to review facilities and procedures and create a more effective operation.

Crisis management after disasters

Unlike most crises, disasters cannot be managed as such, but the catastrophic changes they create might be ameliorated through crisis management. Recent events such as 9/11 and other such incidents in Spain and the UK, as well as natural disasters such as earthquakes, floods and tsunamis, have taught that all that has been said in this chapter so far in relation to planning, training, communication, leadership and team building applies, but in even greater measure, to managing the aftermath of such disasters. Management and their teams cannot prevent such occurrences, so they have to ensure that the proper systems are in place to rescue people and assets and to try and rebuild the business.

A lot of organizations, both governmental and NGOs, have published advice on how to deal with terrorism and its consequences. In the USA, the Department of Homeland Security has published advice for business on their Ready Business website (www.ready.gov/business/index.html). In the UK the internal security service, MI5, has published recommendations: *Protecting Against Terrorism* (Security Service MI5 2006) and is linked to the UK Government's initiative Preparing for Emergencies (see www.preparingforemergencies.gov.uk) which also includes advice on other matters such as avian flu and drought. This in turn is also linked to the Government's UK Resilience website which is run as a news and information service for emergency practitioners by the Civil Contingencies Secretariat at the Cabinet Office. There is also a special website for London as a defined terrorist target (www.londonprepared.gov.uk) prepared by The London Development Agency and Visit London, the local tourism department.

Britain is not often subject to natural disasters although flooding emergencies have recently been on the increase. Again, government agencies and NGOs have issued advice – see, for instance, Business Link's Protect Your Business From Flooding (www.businesslink.gov.uk). Companies have to be continually up to date on planning for possible disasters that might affect them in the future.

Business continuity planning

The UK's Confederation for British Industry (CBI) has also published advice for businesses: *Contingency and Security Planning* (CBI 2006), where the issue of business continuity planning is specifically set out as follows:

- *It is critical that continuity plans are regularly reviewed and tested.* This should be done once or twice a year, across the whole company.
- *All staff should be trained to execute the crisis management plans.* Staff need to understand where the evacuation points are, their role in the event of an incident, who is the in charge, and where the operation's back-up locations are. Most importantly, staff must have easy access to the plan and key contact details.
- *Consider the operation's position in the immediate aftermath of an event.* Does the property have the equipment and the facilities available on site to protect and tend to staff and guests? Companies should consider designated shelters where evacuated staff and guests can assemble. One shelter should be at the heart of the business premises, to protect staff and guests against a bomb attack, with another, more distant shelter, in case of fire or evacuations. These will need to be equipped with food, water, communications and sanitation, and should be big enough to accommodate both staff and guests.

- *Is there a separate location to go to, to continue operations?* If so, its location should be considered carefully – much will depend on the nature and location of the business and the potential threat. If chemical or biological weapons were being released in the city centre, it would be vital to find a relocation site upwind from there.

Crisis management: opportunities for change

Faulkner (2001) quotes Berman and Roel's (1993) description of reactions to the 1985 Mexico City Earthquake:

> '*Crises bring about marked regressions as well as opportunities for creativity and new options. They are turning points in which regressive tendencies uncover discrimination (and) resentment about ethnic and socioeconomic differences … yet they also trigger progressive potentials and solidarity*'.

Examples of opportunities to positively affect the variables include:

- Narrow the service concept: an opportunity to reinvent the product for today's/tomorrow's markets/(re)differentiate your product;
- Refocus markets: if a crisis or disaster has reduced access to certain markets, use the opportunity to attract different market segments;
- Resize: reduce your organization to a more manageable size in the circumstances until new opportunities present themselves;
- Relocate: to a safer environment;
- Simplify processes: use the situation to review all processes and simplify/automate them;
- Combine activities and/or departments for more effective management/better customer service/cost control;
- Update assets: in line with market expectations;
- Redefine staff needs and skills: in line with the new priorities;
- Retrain staff: to better cope with the existing situation or the new direction.

The extent to which companies may take up such opportunities depends very much on how dynamic they are. Those that are better at facilitating change as an inherent part of their culture will be better both at managing crises and at exploring new avenues for their businesses.

Summary and conclusions

In January 2008, John Holmes, the United Nations Under-Secretary General for Humanitarian Affairs and Emergency Relief Coordinator wrote: 'In 2006, 426 disasters affected 143 million people and resulted in $35 billion in economic damage. The number of floods and related disasters was 43% greater than the 2002–2004 average…. All but one of these disasters resulted from extreme weather' (Holmes 2008). Crisis management is now an important concern of management, not least in the hospitality industry as it is vulnerable to many crises (e.g. food poisoning) and attacks (due to drugs, alcohol, gathering of groups of people in a limited space, easy access and egress). Best management practice, added to specific planning, training and communication skills and the involvement of expert third parties can prevent the worst effects of such incidents.

References

Berman, R. and Roel, G. (1993) Encounter with death and destruction: the 1985 Mexico City earthquake, *Group Analysis*, 26, 81–89

Campbell, R. (2005) *Emerald Now … Management Learning into Practice. The Role, Scope and Goal of Crisis Management*, Spotlight on Ross Campbell, Retrieved on 12 October 2007, from http://www.emeraldinsight.com/info/about_emerald/emeraldnow/archive/dec2005spotlight.jsp

CBI (The Confederation of British Industry). (2006) *Contingency and Security Planning*, Confederation for British Industry: London

Faulkner, B. (2001) Towards a framework for tourism disaster management, *Tourism Management*, 22, 2, 135–147

Holmes, J. (2008, January 3) Disasters are the 'new normal', *USA Today*, p. 13A

Jones, P. (2003) Review of Hall, M. C., Timothy, D. J. and Duval, D. T. (Eds.), Safety and security in tourism: relationships, management and marketing, *Journal of Hospitality and Tourism Research*, The Haworth Press Inc.: London, 29, 2, 279–281

Santana, G. (2003) Crisis Management and tourism: beyond the rhetoric, In Hall, M. C., Timothy, D. J. and Duval, D. T. (Eds.), *Safety and Security in Tourism: Relationships, Management and Marketing*, The Haworth Press Inc.: London, 299–322

Security Service MI5 (2006) *Protecting Against Terrorism*, MI5 National Security Advice Centre (NCAS): London

Selbst, P. (1978) In Booth, S. A. (1993) *Crisis Management Strategy: Competition and Change in Modern Enterprises*, Routledge: London, quoted in Faulkner, B. (2001), op cit

Ucelli, L. (2002) The CEO's "how-to" guide to crisis communications, *Strategy and Leadership*, 30, 2, 21–24