

# The Aircraft Bomb Plot

Alleged terrorist attempts to detonate improvised explosive devices on a series of flights leaving London's Heathrow Airport for the United States have provided yet another reminder of the insecure world in which we live and work. Described by Scotland Yard as a plot to commit "mass murder on an unimaginable scale," it underlines the need for businesses to be vigilant and prepared for serious disruptions.

## Security Levels in the United Kingdom

As part of its counterterrorism strategy, the U.K. Government has introduced security levels to enable those authorities and individuals tasked with providing security measures for the public to understand the extent of the threat and provide an adequate response. The "Critical National Infrastructure" group determines security levels through detailed assessments of intelligence, recent events, and knowledge of terrorist networks.

The five levels of threat are broadly categorized as "Low," an attack is unlikely; "Moderate," an attack is possible, but not likely; "Substantial," an attack is a strong possibility; "Severe," an attack is highly likely; and "Critical," an attack is expected imminently.

## The Events of August 10

A sophisticated plot to target up to 10 flights leaving Heathrow Airport for the United States could have caused an exceptionally large loss of life. As the details of the day's dramatic events unfold and the work of intelligence experts leading up to the successful intervention becomes clearer, so the reality of the threat to U.K. and U.S. citizens becomes all the more evident. Several airlines are believed to have been targeted by terrorists planning to detonate explosive devices simultaneously over the Atlantic Ocean. The devices were to have been carried onto the planes in innocuous containers such as drink bottles. The immediate aftermath has caused confusion and severe delays at many of Britain's airports, as well as airports in the United States.

During the night, the British cabinet's emergency committee, COBRA, met to discuss the potential attack and decide on a strategy. The arrests of 24 people, thought mostly to be British-born, prompted MI5, the British security service, to raise the security level to "Critical," meaning "an attack is expected imminently" (see sidebar, "Security Levels in the United Kingdom").

The events at Heathrow prompted the U.S. Department of Homeland Security to increase its threat level to "Red," a move previously unseen for flights coming into the United States.

Many vacationers and business people experienced major disruptions to their journeys, as security was stepped up and hand luggage forbidden from all flights.

The threat levels in the United Kingdom and the United States are likely to remain high for the immediate future, as authorities search for the support staff, supporters, financiers, explosive experts, the security teams, and trainers associated with the thwarted attack. It is too soon to tell what impact the terrorist plot may have on the public's long-term confidence in flying or on other wider factors such as the strength of the stock market or tourists traveling to and from the United States and the United Kingdom.

One thing is certain: Businesses must prepare themselves for similar events in the future and ensure that they are ready for the likely direct and indirect consequences.

## Lessons for U.S. Businesses

Sometimes, even when faced with dramatic events such as those on August 10, it is difficult for many businesses to comprehend how an attack on a major city or transport system would be of direct consequence to them. The reality is that as terrorists continue to target key components of national infrastructures, they are doing so not just to cause massive loss of life, but also to bring about the maximum possible disruption to suppliers and customers through the breakdown of the targeted infrastructure. Businesses must be prepared.

Coming only a year after the July 7, 2005, terrorist attack on London's public transport system, the events of August 10 demonstrate the frequency with which broader, more significant, and physical threats can occur. Marsh would recommend that clients, particularly those more likely to be directly caught up in a future attempted attack, ask themselves the following questions with regard to safety and security:

- Have we considered and prepared to manage the human impact of the elevated threat level?

*(continued on next page)*

- What about our plans should an incident occur?
- Have we identified the credible security threats facing our organization?
- Do we need to update/upgrade our facility's physical security?
- Do we have the equipment, supplies, and support (trained personnel) to respond effectively to credible threats?
- How complete are our emergency response plans? Have they been reviewed and updated recently? When was the last time they were tested?
- Is our internal staff adequately trained to deal with a security threat or respond to an emergency?
- Do our plans consider an end-to-end recovery solution, including key suppliers?
- In the event of an interruption, will we be able to effectively maintain operations?
- Have we reviewed our emergency response plans with the emergency services?
- Have our security measures been scrutinized by experts?
- Have we put into place the processes to provide clear and effective communications to our employees, regulators, customers, suppliers, and the media in the event of an emergency?
- Do we have an employee assistance plan (EAP) to assist employees and their families if they are victims of a disaster or crisis?
- Have we forecast the predictable consequences of an attack on our business or markets?
- Have we prepared our headquarters staff and executives to provide a response and to quickly adjust to an incident that affects either our company or marketplace?
- If there is a major disruption to travel, have we identified alternative travel arrangements? Do your staff have the necessary support to continue performing their critical functions under alternative arrangements?
- Do we have an effective and tested communications plan in place, to ensure rapid and clear communications with all of our implicated stakeholders?

## Managing the Increased Threat

When contemplating how best to deal with security, emergency response, business continuity, and crisis management, companies should consider undertaking a number of related activities, including a threat and vulnerability analysis to determine if the facility has the required physical security. In addition, a security gap analysis can be an effective tool for identifying and eliminating areas for potential security breaches.

Management should communicate with employees about emergency response, evacuation, and accountability procedures and should test plans frequently enough to ensure employees

are aware of safety systems and exit procedures. It is essential that managers reach out to police and the emergency services to ensure plans are properly integrated with a familiar line of communication established in advance of any incidents. In the event of an emergency, it is also essential that personnel know what to do if the police and emergency services cannot access the facility.

Equally importantly, businesses should understand what their most important business processes are, what the impact of an interruption would be on those processes, and what would need to happen to get them going again. On this theme, it is essential to have business continuity plans in place to ensure that operations will not be disrupted in the event of an emergency.

Finally, communications are vitally important to make sure that the right messages are delivered to your stakeholders. Poor communications can sometimes lead to more damage than the direct impact of the incident. Crisis management plans—for use by senior management—should be in place and tested against a worst-case scenario.

## How Marsh Can Help

Marsh has a large team dedicated to assisting clients in developing, enhancing, and improving their business continuity plans. This includes providing hands-on crisis management planning and training and a full range of services to ensure that our clients' business continuity plans—and the people implementing them—are effective in practice.

We work closely with our sister company Kroll, which has significant experience in background screening to identify and eliminate potential exposures, plus wide-ranging skills in security-related advice and on-the-ground support to help companies prevent and respond to threats.

For more information on any of these services or advice on your insurance coverage, please contact your Marsh representative.

---

The information contained in this publication is based on sources we believe reliable, but we do not guarantee its accuracy. This information provides only a general overview of subjects covered; is not intended to be taken as advice regarding any individual situation or as legal, tax, or accounting advice; and should not be relied upon as such. Recipients of this publication should consult their own insurance, legal, and other advisors regarding specific coverage and other issues.

*Marsh is part of the family of MMC companies, including Kroll, Guy Carpenter, Putnam Investments, Mercer Human Resource Consulting (including Mercer Health & Benefits, Mercer HR Services, Mercer Investment Consulting, and Mercer Global Investments), and Mercer specialty consulting businesses (including Mercer Management Consulting, Mercer Oliver Wyman, Mercer Delta Organizational Consulting, NERA Economic Consulting, and Lippincott Mercer).*

This document or any portion of the information it contains may not be copied or reproduced in any form without the permission of Marsh Inc., except that clients of any of the companies of MMC need not obtain such permission when using this report for their internal purposes, as long as this page is included with all such copies or reproductions.

**Marsh. The world's #1 risk specialist.®**

Copyright 2006 Marsh Inc. All rights reserved. Compliance #: MA6-10378