Safety Audit

Dr SALLY LEIVESLEY PhD Lond, FRSA, MACE

Issue 1, January 2002

- A REGULAR BULLETIN ON RISK, DISASTERS, BUSINESS CONTINUITY PLANNING -

RISK AND BUSINESS CONTINUITY STRATEGIC COUNTER TERRORIST OPTIONS

An Options Series to Stimulate Action in 2002

© DR SALLY LEIVESLEY Consultant in Risk, Extreme Events, Business Continuity
sally@newrisk.com

Abstract: The Options Paper suggests a strategy for UK business, which involves establishing a contact point with the Cabinet Office Civil Contingencies Secretariat, broadly based counter-terrorist training involving public and private sector exercising, leadership meetings and loss recovery case study reporting. The objective in 2002 is to harden national business infrastructure against terrorism and extreme events by increasing capability.

SUGGESTED STRATEGY FOR BUSINESS CONTINUITY

1. Request discussions on a central coordination link with the Cabinet Office Civil Contingencies Secretariat to address the planning and recovery of vital services for private sector critical infrastructure and to define responsibilities.
2. Create several recognised points of contact or expertise for large and SME businesses across all industry sectors, including organisations significant for meetings within commerce, directors and professional bodies covering computing, accounting, law and other functions.

   Link traditional professional, tertiary and government course providers to create a national training taskforce for counter terrorist continuity systems and extreme event management. Specialist seminars, capability testing exercises and modular courses would harden the business infrastructure. Flexibility within training content would mean new technical information could be inserted into training in response to threats e.g. anthrax in postal services.
3. Create leadership meetings for Leaders of cities, Directors, Chief Executives, Company Secretaries, Safety/Security/Risk Managers and Auditors. Representatives at these meetings from the public sector including, energy, telecommunications, police and the security services, would assist in the establishment of extreme event policies and practical steps to combat terrorism.
4. Present loss and recovery case studies to business in the aftermath of any global attacks. Case Studies from New York and any corporations that become victims of terrorist threats or major attacks can be placed online and used in training sessions to transfer knowledge and skills in combating terrorism and extreme events.
5. Commence, as a matter of priority in 2002, these strategy options to harden critical continuity functions within the private sector and enhance national security.

BACKGROUND

Globalisation of Terrorist Capability

The strategic options provide to the private sector a risk management capability to harden business and to withstand extreme events such as the Twin Towers attack. Al Qaida, RIRA and other terrorist groups have responded to globalisation by operating through international contacts and utilising information that was previously difficult to access in relation to weapons development.

With this globalisation the different groups are operating in various ways to perpetrate a form of economic terrorism. The economic interests of the USA, UK and other countries have become targets. Activities that were previously limited to national and some transnational boundaries can now affect the balance of world markets.

The terrorist threat of previous decades has been replaced by operations that attack sensitive pillars of the modern economy. Airlines, shipping, financial centres, nuclear power stations and buildings symbolic of economic or religious power are possible future targets that have been identified within the media. Al Qaida is one of the threats to the UK economy, although superficially analysis would suggest that it is second to the currently acknowledged RIRA threat.

A potential impact of the Al Qaida threat is on international business, in particular, airlines and associated insurance sectors. Any subsequent attacks on these sectors could threaten their viability. Secondary impacts from this form of economic terrorism, if carried out on American targets, could still be devastating to Britain if there is a global loss of confidence in the financial market.

These extreme threats cannot be offset by traditional business continuity planning in the United Kingdom which has concentrated on relocation of business and the management of hot or cold sites to replace blown apart buildings. Globalised terrorism and attacks on critical economic pillars, especially financial sectors, will require a sophisticated, responsive and multifaceted business continuity strategy.

Risk Management and Capability Testing

The question addressed by the five strategies listed above is:

How to ensure continuity in 2002 and beyond when unforeseeable extreme events can affect global industry sectors and confidence in business?

The Times, December 19, 2001 quotes Dennis Rumsfeld, US Secretary of Defence:

"We need to face the reality that the Attacks of September 11 – horrific as they were – may in fact be a dim preview of what is to come, if we do not prepare today to defend our people from adversaries with weapons of increasing power and range."

Risk management has for too long focused on threat analysis and the identification of foreseeable events. The methodology has been managed poorly across industry and has failed to establish the much vaunted 'world's best standard'.

There are signs that risk management in the defence sector is changing from assessment of blue sky scenarios to much more soundly based measures of capability. For example, the US Quadrennial Defence Review has concentrated on capability rather than threat assessment. (CNN 27.12.2001)

This is a lesson in strategy that the US would have had reinforced most recently through the loss of the Twin Towers. Probability analysis and threat assessment do not help countries survive the 'unthinkable' attack or protect business against losses of critical functions that can cause an ultimate collapse. The survival of critical functions and the global economy depends on the inherent strength of structures and organisational capability to withstand losses.

Business continuity is therefore a set of actions directed at the immediate and longer term survival of the business interest, regardless of any form of extreme event and which recognises flexibility in business goals and outputs.

Survival can be managed through strategies that allow changes in the products, the locations of business, the clients and relationships with governments and suppliers. Sophisticated and complex systems for the survival of business decision-making (based on Doomsday system planning for the maintenance of critical communications links between decision makers and the holding of key survival data in low threat locations) are now required to meet the threat posed by extreme events such as the Twin Towers attack.

Following severe losses to an economy, businesses may need to redesign their services and products. The essential planning for the survival of people, products and the key capabilities of the business is the function of a business continuity programme.

An example of the need for business continuity and restructuring is currently the reinsurance sector of the insurance industry which has traditionally covered terrorist attack losses. An immediate response to September 11 has been for governmentsto be become insurers of last resort. A more permanent business continuity arrangement could (theoretically) be a new form of catastrophe bond that separates out extreme event reinsurance from other insurance cover. This new product, managed by the industry would ensure business continuity although the form of insurance would be different to that offered prior to September 11.

Critical Infrastructure Protection

Critical infrastructure protection has been a consideration of many governments since the September 11 attack. Governments have concentrated on the public sector with limited inclusion of private sector companies. This means that there are many areas of SME and major business that are not considered in government planning for extreme events.

The private sector, alongside public services, requires some consideration in relation to maintaining its critical functions and the recovery of business functions after any extreme event. The natural leaders for business continuity are the industry representatives within each sector.

Industry leaders can create key linkages with other sectors and with government for the coordination of continuity planning and recovery post-event. These linkages need to be encouraged at the national level in order to create a national capability for the coordination and prioritisation of resources for recovery to the business sector.

Protection of critical private infrastructure therefore requires some actions:

Step 1.

Recognition by Governments of the Dual Risk to Private and Public Sectors from Extreme Events.

This requires the establishment of a contact point for coordination of the private sector. A contact point would provide threat related information, discussion of priorities for recovery and the provision of links with government-protected critical infrastructure such as telecommunications services. A co-ordination point in the United Kingdom, could logically be co-located with the current critical infrastructure protection offered through the Cabinet Office, Civil Contingencies Secretariat.

Step 2.

National Continuity Training and Testing – Policies and Practice

Planning and support by private and public sectors of a nationally focused training and capability testing effort would enhance the nation's strength in counter terrorist response. This could be led by the training bodies within industry sectors, tertiary sector providers and government providers. The focus would be applied skills in continuity preparedness for extreme events.

Training in this form can be easily achieved through modular courses that appeal to cross sections of industry and government. The extension of such courses to exercise tests of capability would provide opportunities for public and private sector bodies to cooperate in testing preparedness for extreme events. Exercise testing and training could focus on major industry losses, information technology infrastructure, and coordinated responses by companies, police, security services, emergency services and local authorities as well as reputation management within the media.

This effort would be a loosely coordinated and linked arrangement with leading organisations taking responsibility for relevant training and capability testing exercises between industry sectors. It would not require a new structure for training or exercising but would encourage as a national initiative many leading educational and training organisations to participate in regular counter-terrorist and extreme event training and testing. Government and private sector providers could agree on standards and methods for the training to ensure that the skills transferred from training would be sufficient to respond to a terrorist threat.

The introduction of structured training for a broad national security capability within the public and private sectors in response to major threats was the subject of the paper prepared for an Risk and Security Management Forum special seminar at Bramshill in 1995, 'Security into the 21st Century' (Leivesley, S, March 1995, unpublished paper). The Paper proposed that:

i. Commercial outreach courses be provided as an in-service training component for police, local authorities, and safety personnel in industry and risk managers in commerce.

ii. There be research and development to exchange information, technology and systems between the private sector and defence. The objective being to protect the population from a range of incidents by systems of preventative and proactive intervention.

iii. That security be brought more into the open through tertiary training. The objective being to provide a raison d'etre for security services through a Security Service which visibly protects the population alongside its covert operations.

iv. That indirectly, the opening up of the Security Services can successfully link defence to initiatives in peacekeeping and population protection …and provide inputs into defence training to create a new flexibility.

The primary objectives behind the proposed system for exercising capability in 1995 were:

_ Counter-terrorist protection of the population _ Protection of Business and Industry _ Prevention of Incidents

Policy support from Government was identified as the key to national training :

'By demystifying the security system and having an unaligned educational structure there is the capacity to develop greater security strengths throughout the country. The cost is not borne by the government but by the business plans of the educational institution. Allocation of liaison personnel as key point contacts for police or other groups allows a degree of information to move directly from government to the private sector.

A Cities and Regional Programme was proposed for focusing on risk management by local authorities, industry and the emergency services. The groups need to have coordination, training and opportunities to exercise together and to follow a common policy. The focus on security management is broadened if training supports the requirements of networks such as Neighbourhood Watch, hazardous industry, local authorities and representative organisations of business and industry.

A Cities and Regional Policy was proposed to establish the concept of self-help at the local level through government encouragement of training in security and risk management. Within industry and commerce, the need for self- help in protection against terrorism has already evolved – the problem is that a patchwork development of self- protection does not provide full security throughout the country. Under situations of threat, a national policy approach covering cities and regions with requirements for risk management is preferable to other approaches where haphazard successes tend to be with the more highly motivated industry and business sectors.

The community network is, in the final analysis, the best way of motivating and persuading local authorities and industry to pay more attention to security. There is also an element of media linkage to inform the public and obtain cooperation.

These suggestions in 1995 apply today, to the extreme threat scenarios that confront government and the private sector in 2002. In two papers to be completed early in 2002, a series of actions to meet the terrorist threat and the management of extreme event risks and structures for planning will be discussed.

Risk and Business Continuity, Strategic Counter Terrorist Actions

A second paper in the Options Series, to be presented February 2002 _ Risk and Business Continuity, Strategic Counter Terrorist Plans, a third paper in the Options Series, to be presented later in 2002

The Author: Dr Sally Leivesley read for a PhD at the University of London based on research into major loss events. She has trained with the Home Office as a Scientific Adviser in nuclear, chemical and conventional explosions and in advanced radiobiology. She has specialised in risk, business continuity and extreme events. Operations covering risk and business continuity in industries since 1976 include: banking and financial services; media; bulk storage; shipping; rail; retail; coal, gas and fuel- oil power stations; petrochemicals; gas; underground and open-cut mines; pharmaceuticals and food manufacturing. She has worked extensively with media teams in exercising extreme events and news coverage. Assessments have been made of the Channel Tunnel, the Thames Barrier, and reports have been prepared following Chernobyl and Three Mile Island. She provided a workshop on the Twin Towers attacks to CompSec2001. In 1997 she exercised an American multinational manufacturer on loss of global headquarters from a 727 flying into a tower building and in the past five years has undertaken anthrax and chemical exercises with critical facilities and companies.