Are you prepared for the worst?

In September three years ago, the world stood still when Al-Qaeda suicide bombers launched a tragic assault on the World Trade Centre in New York. Today, in the light of bombings in Istanbul and Madrid, the threat of terrorism hangs ominously over Europe and European corporates. How can they protect their businesses against unprovoked, unpredictable attacks? Liz Salecka reports.

Graham Wood, then Group Treasurer of Powergen, was in New York on September 11. Accompanied by two colleagues, he was leading a US-wide roadshow to promote a billion dollar capital markets issue.

"We came out of our first meeting just after 9am and were told by our driver that a plane had just crashed into one of the Twin Towers," he recalls. "Then, when we were on the way to our second meeting, which was next door to the World Trade Centre, the second attack happened.

"We were planning a presentation to investors but they were all leaving when we got there. Across Manhattan there was all this smoke.....you just knew a tragic event was happening."

And he continues: "All the high buildings were being evacuated. Everyone thought the whole of Manhattan was under attack. People were in the streets and did not know where to go."

The events of 9/11 brought Powergen's US roadshow - and its capital markets issue - to an immediate halt.

Graham Wood and his colleagues were left stranded in New York, sharing a hotel with firemen working on the scene of the tragedy, with little chance of securing a flight home. Days later, they accepted the offer of seats on a private jet from Montreal back to the UK.

They were back in New York to conduct the same roadshow only two weeks later. The fixed income markets had proved more resilient to the events of 9/11 than the equity markets, and the capital markets issue went ahead as planned.

TERRORISM SPREADS TO EUROPE. For companies based in downtown Manhattan, 9/11 caused a tragic loss of lives, loss of buildings and office accommodation, severe interruption to communications and, from a financial perspective, disruption to the equity and bond markets, and cashflows. Those companies that fared well in the aftermath of the disaster were those that had planned against 'unforeseen incidents', driving home the importance of effective business continuity and disaster recovery planning.

Today, that need is all the more pronounced, not only for corporates in the US – but for major European companies and financial institutions.

In November 2003, Istanbul suffered bomb attacks on the British Consulate and the HSBC bank headquarters in the city, with the loss of several lives, severe damage to buildings and much of the city's telephone network cut off. Then, in Madrid earlier this year, powerful explosions ripped through early morning commuter trains – again the workings of terrorist groups.

Leading business continuity experts now believe that Europe's capital cities - and key financial centres – such as Frankfurt, Luxembourg and Brussels, and London in particular, represent prime targets for terrorist attacks.

In November last year, Control Risks Group lifted London's risk rating from "low" to "medium", a move that coincided with the UK's Home Secretary call on the country to be "in a state of heightened readiness".

PLANNING AGAINST ATTACK. Many major corporates and financial institutions working across Europe have already responded to the political climate. More attention is now being focussed on business continuity management (BCM) – management processes which identify how a business will be impacted by an adverse event and provide suitable frameworks for resilience and response.

"Organisations are looking right across their entire supply chains and at their business continuity plans within this context." says Phil Alcock, Senior Consultant for Business Continuity at Control Risks Group.

"An adverse incident can affect every facet of an economy - and different sectors of the economy will respond in different ways – therefore, you have to look at all your suppliers to judge how you may be impacted."

And David Hughes, Partner, Enterprise Risk Services at Deloitte, adds that larger companies are focusing on BCM, not only because of the threat of terrorism, but because it is now considered an integral part of corporate governance.

"If you suffer an adverse event, you may experience an immediate financial downturn – therefore, regulators are also, increasingly, looking for good controls inside a business," he says. The financial sector, in particular, has taken major strides forwards in implementing business continuity measures in response to regulatory and legislative requirements such as those imposed by the Financial Services Act in the UK.

NOT AN IT ISSUE. The scale and breadth of current day threats to business continuity is such that corporates are also strongly advised to ensure BCM does not remain the sole preserve of the IT department.

"In the past, the IT department was the main driver...or it was the finance director's responsibility," says Hughes. "But BCM must now be seen as a senior management issue because it has implications for the organisation as a whole.

"It should pull in all the skills and competencies across an organisation. There is no set template as to who it should involve but the IT department, facilities, treasury, human resources and media relations are all important."

And he adds: "It is definitely something that a company's corporate treasurer should be involved in."

While experiences vary from company to company, many treasurers are already taking a definite interest in their organisations' corporate-wide BCM planning. Andy Longden, Group Treasurer of the oil and petrochemicals group Shell, points out that he is "a firm believer" in business continuity planning and always takes an active involvement in the drafting and testing of such plans.

"Group Treasury has been involved at a very high level in corporate-wide planning. We are also very involved in the very important process of testing," adds John Westby, Group Treasurer of financial group Aviva – which encompasses the former Commercial Union – the target of an IRA bomb in London in 1992.

WHAT IS BCM? But what exactly constitutes business continuity management? And what are the key considerations that must be made when drawing up business continuity plans?

The services available from leading providers do vary, but experts define BCM as a total end-to-end solution that involves threat assessment and impact analysis; drawing up plans to deal with an incident and mitigate its impact; and longer-term disaster recovery planning. As such it encompasses all the key activities readily associated with contingency planning including crisis management, emergency planning and disaster recovery.

Sungard Availability Services identifies four key stages in BCM – business impact and risk assessment; the creation of well-documented

BCM in treasury

With cash considered the lifeblood of all organisations, leading experts agree that companies must take every step possible to ensure effective business continuity plans are in place for their treasury operations.

And it is vital that treasurers seek to convince their senior management of the importance treasury operations should command in a corporate business continuity plan. "The business needs to understand the impact an incident can have on the treasury function and the treasurer must put a strong case forward," warns Control Risk Group's Alcock.

"There are few parts of an organisation that have to be operational continuously to the same extent as treasury.

"If the treasury function is not there – this will affect the balance sheet directly and other parts of the organisation won't be able to operate."

Short-term liquidity is key. In the event of a disaster or terrorist attack, treasury operations must be quick to resume the management of their payments and, more specifically, receivables to ensure short-term liquidity. Moreover, treasury operations are time-critical – they cannot come to a standstill for days as missed repayments on debt, non-payment of invoices and, in the worst-case scenario – the untimely payment of dividends to shareholders – can result in loss of reputation and credit downgrading.

"Companies often think that preservation of their core product is a priority but, in the short-term, revenue maintenance is the most important thing," says SunGard's Ron Miller, identifying payment of wages to staff and invoicing as the next key considerations.

This is correlated by the group treasurer of a leading European company in its sector: "A lot of damage can be done very quickly if cash inflow is stopped. Billing and collection is vital."

And he continues: "A lack of short-term liquidity can be very damaging, very quickly – this ultimately led to the demise of Enron."

People are a vulnerability. For these reasons, treasurers must focus their attention on protecting the three key elements that the continued operation of their departments depends upon – people, facilities and systems and communication/relationships with third parties and other departments.

As members of their companies' senior management teams, treasurers are frequently subject to the same precautions when travelling overseas and/or catching the same flights as board level colleagues. When drafting business continuity plans for their own departments, people, again, must be the key consideration.

"I was once asked to write a treasury disaster recovery plan that assumed the whole treasury team was dead," says the group treasurer of one leading company, giving a clear indication the importance attached to safeguarding the skills and knowledge of the treasury function.

"And Shell's Longden adds: "People are a key vulnerability... you cannot have a shadow team."

To address people concerns, a treasury operation's business continuity plan must be communicated across the department, well-practised and continuously kept up-to-date.

business continuity plans; establishing the physical back-up facilities required; and ongoing testing and development of the entire plan.

A thorough impact analysis to determine the effect an incident may have on your business is a pre-requisite. Ron Miller, Managing Consultant of SunGard Availability Services, explains that this disciplines companies to find out what the most crucial aspects of their business operations are and who the key people are in terms of their knowledge and the roles they perform. This should dictate the appropriate levels of business continuity that must be put in place.

"You have to do a detailed examination of your business, your people, your systems and your processes and understand what is important. For example, when it comes to data – you must assess how current your data needs to be," he says, pointing out that one requirement here is for organisations to work out what form of data loss their organisations can tolerate. "You also have to define what is a "must" need, and what would be advantageous to have. For example, you need to work out how many people and who you would need at a recovery site – usually only about 25-30% of a workforce is relocated."

Terrorist bombings of commuter trains in Madrid in March this year emphasised the threat to major cities in Europe.

DRAWING UP CONTINGENCY PLANS. A wide range of issues also need to be considered when drafting documents that detail the procedures to be followed in the event of an incident. Such plans should clearly recognise command, control and communication roles. They should identify the core teams of people that will play key roles to mitigate the impact of an adverse event and the activities they will perform.

An important area here is lines of communication – who is responsible for maintaining communication with customers, suppliers and employees in the event of an incident, and via which communication means? Also, who is responsible for contacting next-of-kin, and what are the correct processes for dealing with the media to ensure the risk of any potential damage to business reputation, arising from the incident, is minimised.

Appropriate training must be provided, and awareness of the documentation and its contents spread and communicated across an organisation.

It is also important that such information is not held in one manual kept centrally, but duplicated, and held off-site to ensure accessibility in the event of an incident.

BACKING-UP YOUR SYSTEMS. When it comes to providing physical back-up facilities, companies have to look carefully at their infrastructure, reliance on systems and access to data.

"Each member of the team has a copy of our business continuity plan and knows what to do in the event of a disaster," says Aviva's John Westby. And another group treasurer adds: "You must be able to contact the team out of hours and away from the office.. you must also have practise runs of your plan."

Backing up the treasury. The scale and extent of treasury back-up facilities an organisation requires depends on the size and time-critical nature of the operation itself. Back-up can take many forms, from the simplest – backing up data on disk and holding it off-site – to solutions such as "mirroring" – a method by which data is transmitted in real-time to a separate server on a remote site.

For very large European corporates, use of dedicated back-up sites and systems, that enable treasury operations to be resumed immediately from another location, is the rule – an option favoured by both Shell and Aviva.

Alcock points out that treasurers must also be aware that, for all the benefits associated with centralisation, running a treasury operation from one location does have its risks. "The business case for centralisation needs to look at the risks of being in one place," he says. "If you are part of an international organisation, it makes sense to split treasury operations up so that you are working from more than one site."

This has been the case at Shell, where the centralised treasury operation (see *Refining Shell's Treasury*, p35) is run from three separate centres in different locations – London, Houston and Singapore. The centres, selected for time zone and geographic reasons, use a standard treasury management system, which is fully-integrated, ensuring that each one has total visibility of the group's cash positions and FX exposures worldwide at any point in time. "Being an international group with multiple treasury centres does build in some back-up," says Longden, pointing out that Shell has the option of delegating treasury responsibilities from one centre to another should the need arise.

'I was once asked to write a treasury disaster recovery plan that assumed the whole treasury team was dead'

Communication is crucial. Shell's use of three centres also safeguards the treasury operation against a breakdown in communications with key suppliers and partners – another fundamental aspect of keeping a treasury operation up and running.

Communications with external parties is also recognised as a priority by Westby, who points out that Aviva also has plans to deal with this.

"Plans must include contact names and phone numbers...you have to assume you cannot access your office," adds another leading treasurer.

A final concern, which Deloitte's David Hughes warns treasurers to take precautions against is a dependence on internal departments that are responsible for providing the treasury department with information. "The treasury department is there to support the rest of the business. It is dependant on information it receives from other parts of the business and passing it on," he says. "You have to look at these internal information flow dependencies – if you can't get information from a European subsidiary, what do you do?"

The IRA's bombing of South Quay Plaza in London's Docklands in 1996 was the last major terrorist attack experienced by the city.

Setting up back-up facilities involves making decisions on the level of investment required – from simple back-up of data off-site to fully-equipped disaster recovery sites with appropriate systems and seating for staff. Location and the benefits of ownership also have to be investigated.

"In the past, many London-based companies have had back-up sites in London's Docklands – but if there was a major incident today, it is likely that it would affect Docklands too," says Alcock, adding that distant, out of the city locations should be favoured.

Companies also have to decide between investing capital and resources in their own back-up centres or opting for the services of one or more outsourced services providers. According to a recent survey by IDC, outsourcing business continuity provision can reduce expenditure by 80% and lower IT capital expenditure by more than 20%. "Outsourcing business continuity also releases organisations to focus on their own business," adds Miller.

Finally, keeping a business continuity plan up-to-date so that it satisfies business requirements well into the future should also be considered a priority. For this reason, it is recommended that companies fully test their plans on a regular basis, thereby not only ensuring that they have a working plan but that staff are well versed in its enactment

"There needs to be a continuous programme of activity and the plan has to be exercised," says Alcock. "You need to be aware of the impact that the growth of your business will have on your BCM plans..... A contingency plan must be practical in terms of meeting its obligations."