



Living on the frontline

The resilient organisation

ADVISORY



Contents

| | |
|---|-----------|
| Executive Summary | 2 |
| 1 The resilient organisation | 6 |
| 2 Business Continuity: the way forward | 18 |

Foreword

Since the atrocities of 9/11, Business Continuity has been, and remains, high on the board-level agenda. Increasing global threats now make the resilient organisation a strategic imperative. With reputation, employee welfare and shareholder value at stake, it is a subject no organisation should ignore.

This paper is written for senior executives, with board level responsibility for business continuity, and for professionals with responsibility for the implementation and management of business continuity in their organisation. It provides insight into how leading financial institutions are tackling the endemic global threats of terrorism, pandemic flu and climate change. In the paper, Rick Cudworth, Partner-in-Charge of KPMG's Business Continuity Centre of Excellence introduces the subject of 'the resilient organisation'. The paper sets out some of its attributes, current trends and contains contributions from the Financial Services Authority, HSBC, Morgan Stanley and Société Générale.

KPMG's Business Continuity Centre of Excellence is based in London. It has developed a pre-eminent reputation in the market through its work with many financial institutions and financial regulators across the world.

Executive summary



Failure to make adequate and competent provision for these events could undermine financial stability and threaten the global economy

Resilience: “the ability of a financial industry participant, financial authority or financial system to absorb the impact of a major operational disruption and continue to maintain critical operations or services”

Joint Forum: High-level principles for business continuity

Global risks bring new challenges

Organisations across the world are facing challenges from the global risks of terrorism, pandemic flu and climate change. The likely impacts of these risks are far wider and longer-term than business continuity preparations have traditionally been designed for. As a result, business continuity professionals are facing new challenges.

The financial services sector is particularly vulnerable to these threats given the dense concentrations of major players clustered in high profile centres, its highly inter-dependent supply chain and the strategic importance of the sector. Failure to make adequate and competent provision for these events could undermine financial stability and threaten the global economy. Financial services organisations are ‘living on the frontline’ and therefore compelled to continue to strengthen their business continuity arrangements and create more resilient operations. Fortunately, the sector has always invested in this field and today it is seen as leading the way.

The ‘resilient organisation’ is the ultimate goal

This paper contends that the ultimate goal for business continuity professionals is ‘the resilient organisation’. The resilient organisation will be able to maintain its most critical operations, and ultimately survive all but the most extreme forms of operational disruption. To achieve this, it will:

- Be able to manage the potentially devastating human consequences of events, whilst maintaining critical operations
- Deploy a diverse business continuity strategy for its most critical operations capable of managing local, metropolitan and regional scale events; ‘one solution fits all’ is not an appropriate approach for complex and dynamic enterprises.
- Work effectively and in co-ordination with its main customers, key counterparties, supply chain, the infrastructure providers, regulators and civil authorities

As part of the resilient organisation agenda, this paper discusses managing the people issues, increasing the diversity of business continuity solutions and improving co-ordination with external parties in more detail.



Business continuity is evolving and responding

A number of key trends are also highlighted in the paper, which provide evidence that leading financial institutions are refocusing their efforts beyond the traditional boundaries of business continuity, not only to survive crises stemming from the three major threat scenarios, but to protect and potentially enhance shareholder value in the long-term.

For example, the exercising of business continuity arrangements is becoming more regular, more sophisticated and more connected, both across the organisation and industry-wide. It is a notable feature that business continuity in the sector has, in recent years, become increasingly co-operative; the bar is being raised as a direct result of collective knowledge sharing. Nonetheless this does not diminish the underlying competitiveness of organisations as they seek to maximise the value of their investment, contain 'recovery workspace' costs and position themselves to seek commercial opportunity when a disaster strikes.

Flexibility and simplicity are key

However, whilst these complex issues and challenges must be addressed, our overall premise is also a straightforward one – flexibility and simplicity must be at the heart of successful business continuity. Arrangements must be integrated into the everyday business and look outside as well as inside the organisation. They must be regularly tested to ensure that they remain relevant, that staff are familiar with what is expected of them and updated to take account of changing threats, changes to technological sophistication and changes to the business.

Business continuity professionals must broaden their reach

To achieve the ultimate goal and enhance the reputation of business continuity within organisations, business continuity teams must embrace multi-disciplinary skills; recognising that it is the ability to pull together specialists from a wide range of subject areas combined with a deep understanding of how critical business areas operate that adds real value.

Through a multi-disciplinary approach, there is also an opportunity to integrate operational and financial crisis management under a common framework for decision making, planning and regular exercising.

The financial sector must hope for the best but prepare for the worst

CEO Questions So what?

- Are we proactively investing at the right level to ensure that our business continuity arrangements consistently meet good or leading practice?
- Have we made proper provision for rigorous testing on a regular basis?
- Are our business continuity arrangements sufficiently flexible and robust to cope with changes in demand or staff unavailability after a disaster?
- Can we transfer our critical operations to another geographical location quickly, seamlessly and without disruption to key services?
- Do we actively participate in sharing information and experience with other firms, regulators and civil authorities to ensure an effective, collective response to any incident?

Regulators have a pivotal role

The financial sector must hope for the best but prepare for the worst. Regulators across the world are increasing their levels of scrutiny, but they also have a key role to play in bringing organisations together, encouraging and promulgating good practice and helping set consistent standards and expectations across the globe. The UK Tripartite Authorities, led by the Financial Services Authority have shown the way in promoting a world leading programme of benchmarking and market-wide exercises. The Association of Banks in Singapore together with the Monetary Authority of Singapore have followed suit, with an industry-wide exercise of their own.

Collective resilience is fundamental

In a highly clustered, highly inter-dependent industry, no organisation is an island! By adopting the attributes of 'the resilient organisation' discussed in this paper, organisations will in turn make a significant contribution to the overall prize of 'collective resilience' across the financial centres of the world.

1 The resilient organisation



In the face of global threats, building the resilient organisation is a business imperative

Leading financial organisations have invested substantially in business continuity over many years. However, the days of coping with short-term, isolated threats are over. Now, faced with endemic global threats, the emphasis is changing: ‘the resilient organisation’ is becoming the ultimate goal. But what does ‘the resilient organisation’ mean?

1.1 The resilient organisation

The resilient organisation will be able to maintain critical operations or protect its ‘franchise’ in the face of all but the most extreme events. To achieve this, it will:

- Be able to manage the potentially devastating human consequences of events, whilst maintaining critical operations
- Deploy a diverse business continuity strategy for its most critical operations capable of managing local, metropolitan and regional scale events
- Work collectively and in co-ordination with its main customers, key counterparties, supply chain, the infrastructure providers, regulators and civil authorities

Whilst these are complex issues, flexibility and simplicity are essential. The resilient organisation will be able to take the right decisions at the right time, based not on rigid instructions contained in a detailed manual, but on tried and tested alternative ways of working.

In these organisations, business continuity professionals will have, or have access to, multi-disciplinary skills, take part in knowledge sharing across their industry and beyond, and co-ordinate their planning and testing activities with key external parties.

In the event of a disaster, these organisations will see a return on investment, with their share value outperforming less effective responders. Even without a disaster, their drive for resilience will create more efficient and cost effective business continuity arrangements; reducing the overhead of recovery workspace and detailed plan maintenance by exploiting technology and developing common processes locally, regionally and across the globe.

In the face of global threats, building the resilient organisation is a business imperative but also a long term game; to succeed, it must be embedded in the strategy and decision making at top levels in the organisation.

1.2 Three new challenges come top of the agenda

In the evolution towards ‘the resilient organisation’, and building on business continuity preparations to date, there are three mutually dependent challenges which now need to be addressed:

People: The complex but vital response to people-related issues, including accounting for employees, visitors and third party workers at the time of disaster, understanding the balance of corporate and individual responsibilities, having the flexibility to manage changes in demand in the immediate aftermath of a major disruption and dealing with the human impact of large scale disasters.



Diversity: Exploiting technology and common global processes to achieve greater diversity in alternative ways of working for critical business operations. The high concentration risk of most financial institutions' operations must be offset by improved diversity, whether this is through the sustainable transfer of operations, split-site operations for larger critical functions or successful implementation of remote working solutions.

Coordination: The ultimate success of an individual organisation's business continuity capability is more dependent than ever on its counter-parties, the infrastructure providers, regulators and the civil authorities. Greater emphasis is needed on liaising, planning and exercising with external organisations as business continuity starts to look outside as well as inside the organisation.

1.2.1 The human factor: people come first

At a recent session of several international regulators the comment was made that 'business continuity is not only an information systems issue, but also a human resource issue'. It has perhaps taken events such as 9/11, the July 7 London bombings as well as Hurricane Katrina to move attention to the human factor.

In the financial sector, business continuity has focused historically on information systems and workspace recovery. However, far greater emphasis is now needed on the less predictable and more difficult to resolve, people related issues. This was demonstrated on July 7 when even those firms which were good at accounting for their own staff did not have arrangements in place for accounting for visitors and contractors.

There are five principal areas where greater attention is being placed:

1. Accounting for people immediately after a disaster
2. Effective communications with staff and family members throughout the recovery process – an essential part of any crisis response
3. Developing a clear understanding of where corporate and individual responsibilities lie in given scenarios
4. Developing a better understanding of the human impact of major disasters
5. Increasing flexibility through cross-training in order to resource 'spikes' in demand, which may appear in the aftermath of an incident.

All present and correct: accounting for people

It has become imperative that organisations are able to build a picture of the effect of a disaster on their people quickly and reliably. One of the key lessons learnt from events such as 9/11 and the July 7 bombings was the degree of difficulty encountered by employers in determining whether staff members had been affected.

Many financial institutions are now implementing increasingly sophisticated 'call-out' systems. Some of these systems are capable of providing multi-channel alerts using voice, SMS or email, with the systems automatically logging staff as 'unaccounted for' until a response to one of the alerts is received. Indeed, KPMG has implemented such a system for the entire staff of the UK firm and have integrated it with its Peoplesoft HR system through a weekly update interface.

By providing multi-channel communications capability, the systems partially overcome one key limitation - reliance on the mobile phone network, which tends to quickly become overloaded. Further development of systems in this area is expected. Location notification systems are already available and may be offered to key staff, such as the crisis management and incident response teams, enabling the organisation to rapidly assess the impact on its first-line response capability and gather key people together.



It has become imperative that organisations are able to build a picture of the effect of a disaster on their people quickly and reliably

Case Study

Legal responsibilities of employers and employees in a crisis situation

Anthony Cherry, Partner and Head of Risk Counsel, Beachcroft LLP

The possibility of employers in the financial services industry being held legally liable to any staff who contract avian flu is remote. However, according to Anthony Cherry, partner and head of risk counsel at legal firm Beachcroft LLP, it is important to draw a distinction between liability for avian flu and terrorist threat, where being at work in a financial centre can reasonably be said to increase the risk profile. He points out that under English law such cases usually turn on issues of tort, where demonstrating an employer has done all that is reasonable to meet its duty of care is the basis of defending any claim.

Foreseeability and causation are the two core elements of this duty of care

and are the factors on which any legal case against an employer would be based. "You will never get anywhere with causation issues in the case of avian flu," says Cherry, "There is no telling where someone caught the infection or if work was responsible. In this case employers could demonstrate best practice by following government advice." Unless an employer is active in a sector where avian flu was a greater threat than normal, such as a major turkey or chicken breeder, then there is no case to be made. It is a human resources issue rather than a legal issue. Cherry draws a spectrum from Legionella (otherwise known as Legionnaire's Disease) which can arise as a direct consequence of the maintenance of the workplace water supply and air conditioning, to avian flu where there is no way of establishing causation.

In the case of terrorism the fact of being at work in a city centre office environment does increase the risk. In terms of precedent, 9/11 has had no effect on UK legal position. July 7 occurred when people were en route to work rather than in the workplace and therefore has not created any legal precedent. The explosion at the Buncefield fuel depot (in South-East England, December 2005) happened at the weekend although, had it occurred during working hours, a case might have been built on the decision to locate

a business park in close proximity to an oil storage facility. "In the case of terrorism you have to go back to first principles," says Cherry. "It will always depend on the particular facts of the specific case." In his view it is important to differentiate between a conventional attack and a CBRN (chemical, biological, radiological, nuclear) attack. In a conventional attack the employers would normally wish to get staff out of the building (unless emergency services provide contrary advice at the time) whereas in the case of CBRN they should keep them in the building. All employers in financial services should be aware of the distinction and have correct procedures in place. There is a duty to get that aspect right. In extremis there are issues about food, water and amenities for people kept in a building for a prolonged period, but the key legal issue is whether the employer got the initial decision right. These are largely education and training issues rather than legal matters.

No-one (other than the terrorist) is civilly liable for the terrorist act itself. Questions can be raised as to whether an employer's actions made the situation worse. But Cherry stresses that while good crisis communication is sound employment practice, it is not a legal requirement. "It is very doubtful that a claim for civil compensation could be built on that basis," says Cherry.



With many ancillary services such as catering, cleaning and security increasingly outsourced, the personnel involved no longer count as staff. It is crucial therefore that organisations ensure that the providers of those vital services have comparable arrangements in place to ensure adequate accountability of staff in an emergency.

Now hear this: communications with staff

It is a fundamental rule of crisis management that people must have confidence in what they are hearing. In a crisis it is vital to provide information that is timely, factual, non-inflammatory and not burdensome.

More attention is now being given to staff communications. For example, organisations planning for pandemic flu have tended to pre-prepare communications on travel policy, health and cleanliness and home working. The trigger points for the release of such communications have also been identified. The ability to communicate through multiple-channels, as noted earlier, is also vital. All means available should be considered, from public address systems to pre-recorded emergency information lines, sms, intranet, email or software that will enable web-based, real-time information to be accessed in crisis situations.

There is also a need to focus on internal coordination of communication. This was highlighted during the July 7 terrorist attack on London, when staff in dealing rooms were learning information from the news agencies and the cable and satellite news networks before the business continuity teams were aware of it. The confusion was increased by media reporting of information that was at odds with the intelligence being passed to the business continuity teams from the authorities.

The blame game: corporate versus individual responsibility

The legal responsibilities of directors related to business continuity tend to be overlooked. Effective business continuity requires a proactive approach which anticipates the demarcation of responsibilities prior to the event, much the same way as a properly devised fire drill will mitigate the serious impact of a blaze in a building. Regardless of the jurisdiction, expert legal opinion contends that the two primary issues concern negligence and due diligence.

Shock and awe: psychological effects of a wide scale human impact

Assessment of the psychological impact on staff remains anecdotal. While much was made of the so-called 'blitz spirit' demonstrated by Londoners in the wake of the terrorist bombings on July 7, there is a need for considerably more research in this area. Experience indicates that staff morale is likely to remain high among those immediately involved with the response to a disaster. Such members of staff will take pride in being seen to be actively dealing with an emergency. However, different people will have different personal circumstances, which will affect their attitude and ability to cope. It is also highly likely that the response to a disease epidemic will be much less stoical than in the case of a terrorist attack, given the magnified on-going risk to the individual.

Despite documented cases of employees going to extraordinary lengths to participate in disaster recovery, the true absenteeism rate could hinder recovery and create a significant backlog in processing, from which it can be hard to recover. There is a need for a degree of headroom in staffing levels so that institutions have flexibility. This impacts on the scope of the training procedures put in place to implement business recovery plans. It may be necessary to train much larger numbers of staff than are likely to be needed for a crisis situation, in order to have a comfortable margin for contingencies.

It is a fundamental rule of crisis management that people must have confidence in what they are hearing

Case Study Société Générale

**James Coulson,
UK Chief Operating Officer**

James Coulson, UK Chief Operating Officer for Société Générale, the French financial services group, contends that simplicity and flexibility are the two watchwords for effective crisis management. "The robustness of crisis management arrangements in any organisation will impact upon the speed and efficiency of their business recovery in a crisis situation".

Société Générale believes that the regulator-driven market practices in business continuity that have evolved in the US, particularly since 9/11, are increasingly being adopted as the global standard. These offer a tough benchmark for firms in Europe to work towards. "We undertake a comprehensive risk analysis across all of our businesses to identify which functions and processes are critical to the marketplace and our clients", says Mr Coulson. "We appreciate that the regulators' major

concern is that the failure of some critical systems or processes within an organisation the size of ours could have a wider impact upon the marketplace. Our business continuity arrangements are designed to counter this risk".

Société Générale has a mix of remote disaster recovery sites which can be occupied in the event of a crisis. Some of these are owned whilst others provide dedicated or syndicated seating via third party suppliers. However, the ability to share or switch critical operations between the main business platforms around the world also forms a vital part of the business continuity strategy. "We test our ability to switch critical activities between locations regularly", says Mr Coulson, noting that each location must be prepared for a marked increase in activity volumes if a switch is made. "In reality, the crisis itself may provoke a spike in market activity which may have to be handled by a fraction of the normally available staff". He cautions however, that although there are clear benefits to being able to shift operations instantaneously to other centres whilst remote recovery facilities are brought on-line, it is essential to rehearse the transition from one solution to the other.

Provision for working remotely forms part of the strategy, but Mr Coulson

says it is a challenge to make such arrangements sufficiently resilient. "Whilst we can invest in our own systems and processes so that remote working makes an effective contribution to the business recovery process, we will always have to rely as well on third party infrastructure during a period when this may already be under stress. This gives great cause for concern. Ultimately, the most effective remote-working solutions will be those that are used as part of the normal business platform".

The group has well-developed crisis management plans with a dedicated operations centre for co-ordinating the response to any incident. But for Mr Coulson, effective and accurate communication lies at the heart of crisis management – "a fundamental rule of crisis management is that people must have confidence in the information that they are being given. It is vital to provide information that is timely, factual, relevant and non-inflammatory". This is one focus of the training that Société Générale provides to its crisis managers on a regular basis. The bank also trains three times as many staff as it is likely to need to manage any given situation in order to have real resilience against a crisis which lasts considerably longer or is more extreme than was foreseen.



Although staff members may rally immediately after an event, business continuity planning must take account of the fact that the psychological impact of a disaster on members of staff may only become evident some time after the disaster takes place. Counselling may be required. This is borne out by psychological studies of individuals who were directly affected by 9/11. These revealed that in the medium term after the attack, three quarters of those surveyed experienced depression, nearly half had impaired concentration and a third developed insomnia. Significantly, business continuity preparations must be flexible enough to cope if a significant number of staff are either unable or unwilling to work in the aftermath of a disaster.

Preparing to handle the physical and emotional effects on employees of a catastrophe, including trauma, will be instrumental in achieving long term successful recovery.

Flexibility is essential

When a 'disaster event' occurs organisations are likely to face changes to the 'normal' demand profile. For example, in the period immediately after a sudden major operational disruption, spikes may occur in trading activity which in turn increase demand on back office teams; in a pandemic flu outbreak customers may switch initially to cash and make greater use of telephone or internet banking. These changes in demand will potentially compound the effects of reduced staffing levels as a result of the disaster event itself and create a significant back log. The ability to move available resources or transfer work to help meet changes in demand in the short term must be considered and adequately addressed.

1.2.2 Diversity – 'one solution fits all' doesn't work

Over recent years, many leading financial institutions have consolidated their critical operations, often into large single premises in high profile locations.

While technology has helped these organisations evolve parts of their business continuity strategy, for example, with the short-term transfer of front-office trading to other financial centres, the investment in 'out of town' workspace recovery centres to provide alternative facilities in the event of a disaster has been significant. These centres are typically high in their set-up and maintenance costs and may still be

insufficient in dealing with the wide spread impact of the global threats.

Achieving greater diversity in business continuity arrangements, at least for the most critical operations, is vital. This means exploiting technology and reducing the potential impact of the human factor by deploying two or more alternative ways of working, with at least one of these maintaining a high degree of geographic dispersal.

There are three key aspects to this:

- Greater use of remote working capabilities – although this is often suggested as a solution, there is significant dependence on telecommunications network providers and investment may be required to enhance remote access seats and bandwidth. There are also substantial operational, regulatory and human resource issues to be considered as well as the need to make it 'business as usual' through regular testing
- Setting up split-site operations for some larger-scale critical functions, whereby the same process is run across two or more geographically discrete locations and work load can be readily transferred
- Enabling the transfer of critical operations to other global locations without depending on significant staffing from the affected location – moving the work, not the people



Achieving greater diversity in business continuity arrangements, at least for the most critical operations, is vital

These options are not mutually exclusive or necessarily replacements for secondary recovery centres, but should be viewed as part of a blended mix of business continuity solutions. It is the precise nature of this blend that is proving challenging to organisations as they increase their resilience.

Home alone: remote access working

Following the bombings on July 7, many employees were unable to get to work because the public transportation system was shut down. Under such circumstances, organisations with extended high-speed broadband and secure computer access to key employees' homes for remote operation, have a significant advantage. Additionally, virtual private PC networks, teleconferencing facilities and call forwarding all have a valuable role to play.

While much is made of remote access working as a possible solution in the event of a pandemic flu outbreak, companies must assess the viability in terms of their own operations. It tends to be the case that less business critical functions are more suitable for remote access working, whilst many critical functions such as, for example in retail banking, cash handling and branch operations, by definition require on-site staff. Even critical functions such as payments and settlement and trading provide extreme challenges to remote access working.

Several key points must be addressed to ensure successful remote access working.

- Existing infrastructure - can it support the increased volumes of use and can it be relied upon during an emergency situation?
- IT support functions – have these been checked to make sure they are geared up to handling the switch to remote working?
- External suppliers eg. telecommunications companies – are they able to maintain their level of service provision?
- Systems – do these need to be upgraded to provide additional capacity? If so, the lead times and costs will have to be taken into account.
- IT licences held for the business and financial software – do the existing licences cover the eventuality of home-working or will new licences need to be purchased?

The transfer to home working could have significant implications for system and data security. Existing arrangements will need to be examined to ensure they are sufficient to cover the eventuality of remote access working.

But this is also much more than just a technology issue. Control and compliance issues and regulatory implications will need to be fully assessed, as will the training and testing needed to ensure that staff can make the switch to remote working seamlessly and painlessly.

Provision must be made for key employees to gain remote system access in the event of their being unable to get to the workplace, and it will be necessary to agree in advance which personnel can work from home effectively and who has the authority to initiate these procedures. It is also vital to consider just how far remote working is compatible with the management structure in which the business operates. Finally, the specific health and safety aspects of home-working will need to be taken into consideration.

It is one thing to have the capability for remote working. It is quite another to be able to use it. Successful home-working depends on staff being able to function effectively in this environment. In particular the differences between short-term (ie, days) and long-term (ie, weeks) home-working need to be taken into account. In the long-term, issues such as remote management, a sense of isolation and health and safety issues need to be considered. Firms should test their ability to operate business in home-working mode on a regular basis, say one day per month every month, especially in financial services companies where remote working is not part of the corporate culture.



An increasing number of large financial institutions are able to transfer parts of their operations across the globe at very short notice

Double indemnity: split site operations

Running critical operations concurrently at two or more geographically dispersed sites is perhaps the most effective means of mitigating the impact of a disaster at one of those sites, especially when combined with other business continuity solutions such as transfer of operations or a smaller secondary recovery centre.

Whilst this is against the trend of consolidation and there are substantive cost implications, the significant threat and increased risk level is making such business continuity solutions increasingly attractive for mission critical operations. Split site operations provide a degree of in-built capacity and continued presence, thereby reducing the initial impact of a disaster and assisting in faster and sustainable resumption to normal business volumes. It is important to ensure that the two sites are sufficiently geographically dispersed so as not to be affected by the same event.

Split site operations offer one of the best business continuity solutions for large-scale, time critical, high impact activities. As the regulatory environment and market expectations move increasingly to defined recovery targets, which may include: clearance of all material transactions within the working day; and capacity to trade near normal volumes by the next working day, the pressure to have split-site operations as part of the overall business continuity mix is likely to increase.

Going global: transfer of operations

An increasing number of large financial institutions are able to transfer parts of their operations across the globe at very short notice. This is particularly the case for front office trading operations and has been enabled by the adoption of global systems and common processes, with key business lines managed and operated globally.

Although many financial institutions have the capability to transfer operations, there are a number of challenges that need to be addressed moving forward:

- Sustainability – currently the transfer of a book of business is often viewed as a short term solution, enabling key market exposures to be managed or contained. However, due to resource and system constraints, this may not be sustainable over the medium or long term in many cases.
- Unique Elements – although common processes exist, it is often the case that a percentage of the work performed in one location is unique to them alone. Other territories cannot replicate it, making the transfer of operations a partial solution only.
- Testing – for many organisations, the feasibility of transferring operations has not been sufficiently well tested. Handover protocols, regulatory impacts, use and reconciliation of systems, handling the increase in volumes and back office settlements are particular challenges.

Some of the macro issues regarding the use of common systems, operating models and training of staff will all need to be aligned intra and inter regionally as much as possible to enable the smooth and seamless transfer of operations to become a longer term business continuity solution for the future.

Diversity means staying on the radar screen

Developing diversity in business continuity arrangements will in part depend on exploiting technology to deliver fast, alternative methods of operating critical functions without dependency on staff that may have been directly impacted by the event. Increasingly, this will have to be sustainable over a period of weeks and months rather than merely hours or days.

In practice, the resilient organisation will make best use of several, if not all of these options. The approach of 'one solution fits all' is no longer appropriate. Organisations may take a two or three-tiered approach, using local and 'out of town' recovery centres combined with remote working capabilities, transfer of operations or split-site operations.

Case Study

HSBC

Bob Piggott,
Head of Crisis Management

Bob Piggott, head of crisis management at HSBC, believes that the financial services sector has learnt several crucial lessons from 9/11 - everything from the resilience of buildings and systems, to the implications of having large concentrations of people on one site as a result of consolidation. The international banking group, an early adopter of business continuity capability, has changed its focus as a consequence. Now, particular attention is paid to the instantaneous and seamless switching of business across primary and back-up sites.

HSBC is able to use its global reach to transfer operations from London to New York or from New York to Hong Kong, as required. According to Mr Piggott, the first aspect to consider is the skill matrix: "If we lost, say, an entire derivatives team, we can fall back on our global coverage but there is a challenge. New York has a different system from London and it will have to deal with a huge upsurge in capacity caused by the doubling of normal

business volumes and the extra trading caused as a reaction to the incident." In terms of its people, HSBC believes reliable and effective communication is vital - "in the UK all our staff have a telephone number they can ring to receive an updated status message in the event of an incident," says Mr Piggott, "and evacuation instruction cards are issued to all bank staff as a matter of course". However, the terrorist attack on London on July 7, 2005 happened while employees were commuting to work, highlighting the need to be able to contact people while they are in transit. Provision for this has now been factored into HSBC's plans. The incident response team was called together within 10 minutes of the first bomb going off in London, before the official confirmation of a bomb attack even came through. Another internal communication issue revealed by the attacks was that HSBC's dealing teams were getting reports from Sky, Reuters and media services ahead of the incident team. "What's more, the information the media was providing conflicted with what the police were telling us," notes Mr Piggott. "We have direct communications links to the main authorities such as Transport for London and the Metropolitan Police but our staff were getting a different version of events from television which could have created confusion."

Action to counter that problem of coordinating internal communications to avoid conflicting messages has now

been factored into the continually updated business continuity strategy. Clear communication with all stakeholders is a key element of HSBC's response. The bank's communications team is tasked with getting appropriate messages to key stakeholders such as the media, the regulators, and the Bank of England. Call centres are given a script to keep customers informed.

A good incident management plan must be flexible," says Mr Piggott, who notes that flu pandemic constitutes the greatest risk worldwide. "In such a case there is likely to be high absenteeism which will affect the whole supply chain and infrastructure. We have a group plan, country plans and departmental plans. Our flu pandemic plan is based on us surviving a worst case scenario of 50 percent of the workforce being absent for several weeks." He acknowledges that his figures are higher than government estimates but believes that such caution is warranted. "There will be up to 15 percent of staff off on annual leave at any one time plus there will be sick staff, those looking after the sick, and others who are traumatised."

HSBC has assessed the technical and operational requirements for successful home-working, as part of its preparation for pandemic. Its aim is to have the ability to provide fully for remote working, together with a major test of effectiveness during 2007.



Better analysis of costs and impacts will continue to drive the trend towards greater in-built resilience for the most critical operations, with a diminishing dependence on recovery centres. Greater understanding of the business operations, combined with input from a range of departments including HR, regulation and compliance, technology, property and facilities amongst others is key to achieving the best result. In each case the options and potential barriers for each critical operation need to be identified, prioritised and worked through.

1.2.3 Co-ordination: all for one and one for all

No organisation is an island. Yet most business continuity planning to date assumes that a disaster impacts only the organisation or part of it. Financial institutions are increasingly aware that their business continuity planning cannot deal effectively with a crisis in isolation from the financial, regulatory and civil community at large. Without collaboration, plans not only risk failing but may compromise the response of others around them.

Understanding the degree of mutual dependency and integration with other parties will ultimately determine the success of any individual business continuity plan. With the fungibility of money and consequential systemic risks, a co-ordinated approach is integral to effective business continuity planning in the financial sector.

There are several issues to consider:

- Sharing experience and knowledge with other firms in the sector, through forums such as the Securities Industry Business Continuity Management Group (SIBCMG), to develop an effective, collective response
- Anticipating, and planning for, disruption to the financial services supply chain
- Regular communication with regulators, civil authorities and emergency services to ensure coordinated action
- Participation in market-wide exercises and benchmarking activities such as those led by the Tripartite Authorities and KPMG in the UK.

The global threats that organisations now face are typified by their wide-scale and longer-term impact. Recent crises have clearly emphasised the need to communicate with many parties and take collective decisions. In the event of a major operational disruption, the success of individual plans will depend crucially on understanding the responses of others, including regulators, the civil authorities, transport authorities and the supply chain of critical business partners.

A recent report from the United Kingdom's Tripartite Financial Authorities found that over 40 percent of firms in the financial sector take no account of local authority emergency planning in their own continuity plans, while some 75 percent fail to involve neighbouring businesses.

John Milne, head of business continuity management at the Financial Services Authority, confirms that coordinated exercising and interdependency is the key aspect to business continuity: "In financial services, unlike other sectors, your own business continuity is only as good as that of your counterparties. The industry is working closely with us to develop and pilot the benchmarking and market-wide exercises. The participation in pursuing standard and leading practice is very encouraging."

The supply chain gang: no weak links

The financial sector supply-chain is highly inter-dependent and transactions are often near instantaneous. According to the Supply Chain Resource consortium at North Carolina University, supply chain disruptions caused by events such as 9/11 have negatively impacted shareholder value by as much as 8-10 percent in companies. The impact is greatest in 'time-sensitive' sectors, such as financial services.

Recent crises have clearly emphasised the need to communicate with many parties and take collective decisions

In the wake of the impact of Hurricane Katrina more than a dozen major financial services firms, including Citibank, JP Morgan Chase and Bank of America, together with several leading technology vendors, launched the Resiliency Maturity Model Project to create benchmarks and define terms for business continuity planning across the entire supply chain of a financial enterprise. Commenting on the initiative, Charles M. Wallen, managing executive of the New York-based Financial Services Technology Consortium and the project's director said: "Katrina is one of many large-scale events that reaffirm the need to have strong business continuity plans and to provide a road map for third-party providers to understand what's needed. We have to do a better job at raising the bar."

A further lesson learnt following Hurricane Katrina was that financial institutions can play an important role in facilitating the recovery of a community, region or even state through their involvement with voluntary sector relief programmes and projects. An institution's support of such organisations through its corporate social responsibility (CSR) strategy can act as a catalyst for recovery.

State of emergency: working with the civil authorities

In a major financial centre like London, effective business continuity capability will have factored in the cooperation required from the City of London police, the City of London Corporation, Canary Wharf Management, Transport for London, the London Underground and the emergency services. Typically organisations have tended to overestimate the speed at which civil authorities will provide information to them, for example, on casualties; and underestimate the extent and duration of their response, for example, on cordons.

Account must be taken of the fact that civil authorities must balance the need to inform the commercial world of its likely responses, while not providing information which could be used to undermine the effectiveness of the response. In the case of a flu pandemic it is important to decide the appropriate levels of message and communication to keep people informed without exacerbating any sense of panic.

Safety in numbers: the value of market-wide exercises

The UK financial sector has taken a lead in this area. Under the auspices of the Tripartite Authorities (Bank of England, HM Treasury and the Financial Services Authority) a programme has been initiated to improve the overall state of preparedness of the UK financial sector to respond to a 'Major Operational Disruption'.

In 2004 and again in 2005, KPMG in the UK led a major simulation of a terrorist attack to test the ability of some of the UK's leading financial organisations to continue operating in circumstances that had the potential to throw their business into turmoil. In the November 2005 exercise, more than 3,000 people from 70 institutions were involved. Allowing the key determiners of response (police, transport, government and regulator) to play out some of their actions against a realistic scenario, has enabled banks to conduct a post-exercise gap analysis of their response plans to make them more robust and accurate, specifically in areas of mutual interest such as the stability of markets and the operation of payment systems. In May 2006, KPMG planned and prepared an even larger scale exercise in Singapore and the concept looks set to roll out through many of the other global financial centres.

The very high level of support and participation these exercises have drawn indicate the importance that organisations now attach to testing out their plans in co-ordination with others.

2 Business continuity: the way forward



An effective and holistic continuity strategy is vital to satisfy the regulatory environment and to protect the interests of all stakeholders

With the financial services sector exposed to an increasing level of threat on a global basis, investment in robust business continuity capability is mission critical for all market participants. The compelling evidence from such major catastrophes as 9/11, SARS, Hurricane Katrina and the July 7 attacks on London is that an effective and holistic continuity strategy is vital to satisfy the regulatory environment and to protect the interests of all stakeholders: from employees and investors to clients and suppliers.

In this paper we have argued that the ultimate goal is 'the resilient organisation', and for the industry as a whole, 'collective resilience'. We have defined what is meant by the resilient organisation: one that has a diverse range of business continuity solutions for its critical operations; that is capable of managing potentially significant people related consequences of a disaster; and one that is connected to and acts in co-ordination with its counterparties, infrastructure providers, regulators, civil authorities and its wider community.

Whilst business continuity is becoming more co-operative, it is also a competitive issue; in the event of a disaster return on investment will be maximised by those most prepared. Its direct connection to shareholder value and employee welfare makes it a priority at board level. In this section, we set out further evidence of the validity of the concept of the 'the resilient organisation' by looking at some of the current and predicted trends in business continuity within the financial sector.

Investment will continue to be significant, consistent and pro-active

Investment in business continuity in the sector will continue to be significant, consistent and pro-active, though organisations will be able to contain or reduce costs in some areas as they seek alternative, more diverse strategies which better exploit technology and reflect the globalisation of their business operations.

Historic investment patterns in this field have tended to be reactive, sporadic and driven by response to media reporting of 'disaster' events. This traditional 'boom and bust cycle' was effectively broken in 2001 with the Al Qaeda attack on the World Trade Centre and Pentagon. The sheer scale and impact of this event pushed business continuity to the top of the agenda for government, regulators and those concerned with corporate governance and the protection of employee welfare and shareholder value. Continued terrorist attacks across the world and the emergence of other global threats including pandemic flu and climate change, as well as seemingly more regular large scale local disruptions have maintained the subject's attention and priority over the intervening years.



Perhaps because of the impact of 9/11, the leading financial institutions, together with the regulators, have moved from being reactive to proactive. As a result, over the last few years business continuity strategy has undergone a rapid evolution. With business continuity now recognised as a core competence within many leading financial institutions, investment in this area will continue to be significant, consistent and proactive.

Nevertheless, there will be pressure to reduce the cost of investment in some areas, for example, in what is often seen as 'redundant' recovery workspace. This will lead organisations to seek alternative solutions which exploit the advances and investment made in technology as well as the increased regional and global alignment of many critical business operations.

Change is the only constant

The dynamic environment in which financial organisations operate, combined with the endemic global risk profile will continue to drive changes in business continuity strategy and the need for flexibility and resilience. As part of the drive to increase resilience, there is now greater emphasis on people issues, diversity of business continuity arrangements and co-ordination with external parties.

Changes to business operations – through M&A activity, relocations and expansion – will continue to drive a significant amount of re-engineering of business continuity arrangements.

This highly dynamic environment coupled with the nature of the global threats faced by the sector will also drive the need for flexibility in business continuity arrangements and provide the opportunity to reassess business continuity strategies more fundamentally.

The testing and exercising of business continuity arrangements will be more regular, more rigorous and more sophisticated

Typically organisations will seek greater resilience by overlaying local, metropolitan, regional and global business continuity arrangements. For example, it is increasingly common for institutions to be able to transfer responsibility for open market positions and managing their 'market risk' to teams in other global financial centres very quickly. This is enabled by common global systems, data and processes. The challenge is perhaps to make this practical on an intra-day basis and more sustainable over a longer period and wider ranging across business activities.

The changing nature of global threats is also bringing people issues and co-ordination across the sector to the fore. Pandemic flu affects people, not facilities and technology upon which business continuity arrangements have traditionally focused. In addition, the impact of global threats affects not just one organisation, but many. Because the financial sector is highly clustered and highly inter dependent, the issue of co-coordinating responses and decision making across the sector, as well as ensuring continued connectivity through the supply-chain, becomes a significant challenge.

The three key challenges of resilience, people and co-ordination are dealt with in more detail under 'the resilient organisation' earlier in this paper.

Practice makes perfect

The testing and exercising of business continuity arrangements will be more regular, more rigorous and more sophisticated. In particular, exercises will be conducted not just locally, but intra- and inter-regionally within global organisations, better reflecting the scope of their business continuity strategies. Exercises will also be conducted 'market or industry-wide' within major financial centres to test collective responses and decision making and the inter-connectivity of business continuity arrangements.

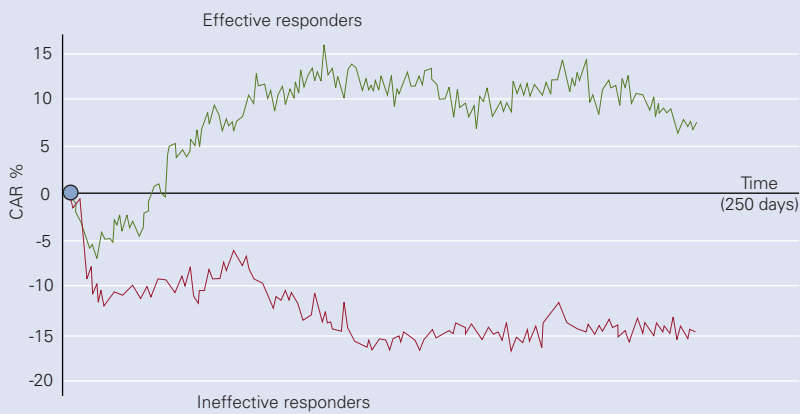
Regular testing or exercising of business continuity plans is essential to ensure their effectiveness and ability to cope with changing business and operational needs. Increasingly, business continuity will become more dependent on well rehearsed practice rather than detailed prescriptive written procedures. Many organisations have found that when a disaster strikes there is no time to refer to manuals, and practice and flexibility are key. As a result, testing will become more sophisticated: in terms of the complexity and depth of the scenarios and the methods of delivery.

Scenarios will contain greater emphasis on short and medium term business impacts and activities. To achieve this, there will be greater integration between operational and financial crisis planning, modelling and exercising. Delivery techniques will simulate (so far as practical) those likely to be used in real-life and exercises will be run locally, intra- and inter-regionally so that regional and global business continuity strategies can be tested out.

In addition to an organisation's internal testing programme, there will be more exercises within major financial centres which are 'industry-wide', involving counterparties, markets, infrastructure providers, regulators and civil authorities. These will involve testing the physical connectivity of alternative arrangements across the sector, as well as key market-wide information gathering, communications and decision making.



Impact of catastrophes on shareholder value



Source: Rory F Knight & Deborah J Pretty, Oxford Metrica, Templeton College, University of Oxford 2005

Cooperative but competitive, as organisations seek return on investment

There will be increased knowledge sharing amongst business continuity professionals which will help raise the bar and drive competitiveness. Organisations will seek to maximise the commercial benefit of their business continuity investment and in the event of a disaster may have little tolerance of less well prepared organisations and therefore be more willing to take full advantage in the market.

Existing research and analysis makes a compelling case for robust business continuity. It also indicates strongly that business continuity is a board level issue due to the potential impact on shareholder value and corporate reputation.



Research first conducted by Knight and Pretty in 1996 (*The Impact of Catastrophes on Shareholder Value, Oxford Metrica*) graphically illustrated the benefit of effective response to a disaster. This comprehensive study analysed the impact of a series of major high-profile corporate catastrophes on the long-term performance of the listed companies in question. Analysis of case studies revealed that the best performers reputation was enhanced and, after an initial dip, their share value rose. In contrast, the poor responders lost up to 15 percent of shareholder value in the long term.

However the contemporary threats to financial services corporations are of a different order to the Knight and Pretty research case studies. By comparison today's threats are at a more macro and global level.

The new generation of threats typically impacts whole communities of organisations. This is of specific importance to the financial sector, uniquely highly clustered as it is around a few global financial centres. Such concentration of major players will inevitably enable the market to be able to identify quickly which organisations have responded successfully as well as those that are insufficiently prepared.

This premise is supported by more recent research by Pretty (*Protecting Value in the Face of Mass Fatality Events, Oxford Metrica*), which concludes that such events 'have double the impact on shareholder value than corporate catastrophes in general'. It also concludes that 'the market makes a rapid judgement on whether it expects reputation to be damaged or enhanced' and identifies 'sensitivity, compassion, honesty and courage' as key factors to which the market responds positively. 'People come first' is one of our defining attributes of 'the resilient organisation'.

Whilst most players in the financial services sector tend not to exploit others' misfortune this could change as more aggressive businesses seek a return on their investment in the immediate aftermath of a major operational disruption. Furthermore, certain leading practice firms, already offer their business continuity expertise as a value-added service for clients, using it as a business development tool.

Nevertheless, the benefits of knowledge sharing between business continuity professionals and the business imperative of co-ordinating decision making at a time of crisis, will mean that the trend towards greater co-operation through formal and informal information sharing forums is likely to continue. Organisations such as the Securities Industry Business Continuity Management Group (SIBCMG) in the UK, which has members from fifteen of the leading investment banks in London, provides a forum for business continuity professionals within these organisations to share information, and importantly to set-up protocols for the co-ordination of response in the event of a crisis. This is likely to extend to other financial centres and across other industry segments.

Greater cross-industry knowledge sharing will be helpful. Whilst the financial sector has done much to lead the way in business continuity, other key industries also have a significant amount of expertise and experience to contribute.



Business continuity professionals must broaden their reach

Business continuity professionals will need to gain deeper understanding of how critical parts of their business operate. Business continuity teams need to include, or have access to, multi-disciplinary skills to properly address the complex challenges they face and help integrate operational and financial crisis management.

Looking at the trends above, the emphasis is now clearly on delivering ‘advanced business continuity solutions’. This needs to be achieved within an often complex, internationally varied and rapidly changing regulatory environment. Tackling these major issues will require multi-disciplinary skills, an understanding of the global regulatory environment and a far greater working knowledge of critical business operations.

The emergence of well-staffed, discrete business continuity teams, with improved connections to operational risk, is an encouraging development of the last five years. Strong regulatory interest as well as the immediacy and criticality of impact are the key drivers in this regard. The sector has also benefited from increasingly effective networks of business continuity professionals, within banks and across peer groups, such as SIBCMG which is helping to raise standards and to a degree, develop a more co-operative yet competitive approach. As a result, there is a high level of collective expertise within the practitioner community that can be brought to bear to deliver the ‘the resilient organisation’ and contribute to overall collective resilience.

There is also an opportunity to integrate operational and financial crisis management; providing a common framework for decision making, planning and exercising. This recognises that a major operational disruption could cause a financial crisis and decision makers may need to deal with both issues simultaneously. It also combines the often complimentary strengths in these two areas: operational business continuity planning and exercising; with financial scenario, impact analysis and stress testing.

Case Study Morgan Stanley

**Richard Deighton,
Business Continuity Manager –
Europe, Middle East & Africa (EMEA)**

Richard Deighton, EMEA Business Continuity Manager at Morgan Stanley, believes that business continuity planning (BCP) has come of age in recent years. He contends that it is now a core and integral part of corporate strategy rather than a peripheral specialist area. From typically being seen as part of the remit of the Corporate Services and Facilities department in the 1990s, it progressed to being deemed an IT issue before being recognised as a key firm management issue as it is currently.

Advances in technology have changed the approach to business continuity. Morgan Stanley has just built a new remote data centre, which allows real-time back-up. This has meant dispensing with the need for a dedicated BCP technology centre. "BCP has to be focused on delivering shareholder value and making financial sense rather than just delivering successful systems recovery" says Deighton.

From being a modest budget item, business continuity is now a major investment for Morgan Stanley. However, much of the expenditure is accounted for as part of day-to-day operational costs of the business rather

than a separate outlay. "As the BCP budget has grown and our way of accounting for it has changed it has become much more visible at board level," says Deighton.

He has witnessed a sea-change in attitudes to BCP since the early 1990s when Morgan Stanley was affected by the bombing of the Baltic Exchange in the City of London. At that time, the focus was very much recovery-driven and technology focused. Investment was highly cyclical with spends going up in the immediate aftermath of an incident and then being scaled back until the next event. "At the end of the 1990s we identified the need to address that," says Deighton. Today, he notes the status and capability of BCP has never been greater, a change confirmed by the appointment of business continuity professionals at the most senior grades (ie, Managing Director) in the US.

However Deighton warns that some firms still regard business continuity as a technology-focused disaster recovery task. "BCP blurs the distinctions between many discreet areas from Human Resources and Security to Technology. The approach has to be holistic." He stresses the need for regular, realistic testing of the continuity plans to keep them relevant and effective. Morgan Stanley runs a series of major tests every year at various levels within the organisation.

Chief among them is the Easter Test. Over the Easter weekend the firm takes advantage of the powering down of all its main data centres in Canary Wharf to run a full simulation of a total loss of data at all offices. Some 200 people are

despatched to the recovery site to run operations from there. This major annual test is supplemented by business process testing twice a year. A team is sent to the recovery site to execute a trade from that location. "It's very important in terms of familiarising staff with everything from getting to the site to knowing how to use it." Separate table-top exercises are conducted to run through a simulation of an avian flu outbreak or a bomb attack. The crisis management and BCP teams run through the plan and test it for weaknesses. There are regular drills for the crisis management teams in which they do everything that would happen in a real disaster from evacuation to physically walking to a recovery site and using radio transmitters for communication so that there is no reliance on the phone. "They have to get used to it so that it becomes familiar."

Delivering value in business continuity is a key focus. "We are doing a lot more with our clients to help them understand BCP. We offer our services as a value-add for clients and in this way it is a business development tool. Monetising BCP in this way makes it less burdensome."

However despite the competitive advantage offered to firms which have leading practice in BCP, Deighton says that collaboration among firms, especially in the wake of 9/11 and 7/7, takes precedence. Through organisations such as SIBCMG (the Securities Industry Business Continuity Management Group) there is more of a drive to share knowledge and experience recognising the mutual dependency of the sector."



Regulators will be proactive and play a vital role

Financial regulators across the globe are likely to be increasingly proactive in their levels of scrutiny, whilst also seeking greater consistency in cross-border regulatory approaches to business continuity. Moreover, many may adopt a key role in helping to bring organisations together, encouraging and promulgating good practice and sponsoring market or industry-wide exercises.

Historically, regulators did not play a significant role in driving forward business continuity within the financial sector. This was mainly because the risk of major operational disruption (MOD) to the sector was seen as a very low probability and thus ranked below other risks – notably prudential and consumer risks – within regulatory priorities.

The tragic events of 9/11 and the series of subsequent high profile terrorist and other incidents have radically altered perceptions of the probabilities associated with MOD. As a result, the regulatory authorities in all of the main financial centres have taken a much more proactive approach to assessing and promoting improvements in the level of preparedness for MOD amongst key financial market participants. In some jurisdictions (notably the US), the regulators have taken a prescriptive approach – for example, in setting business recovery times. Alternatively, in the UK the regulators have taken a non-prescriptive approach, instead preferring to work with the sector on a voluntary and co-operative basis to achieve shared goals.

Under the leadership of the FSA, the tripartite authorities (HM Treasury, Bank of England and the FSA) have rolled out a programme of market-wide exercises and benchmarking – making a significant contribution to enhancing the preparedness of the UK financial sector as a whole. Overall, the programme has resulted in greater understanding of the regulator's role in a major operational disruption, increased confidence in the collective ability of the sector to respond effectively and importantly, brought the industry closer to the civil authorities on whose response they are critically dependent. It has also resulted in increased information sharing, the promulgation of good and leading practice and potentially increased consistency, or at least an understanding of expectations, across the 'supply chain'. This model appears to be attracting significant interest among regulators in other jurisdictions.

Under the leadership of the FSA, the tripartite authorities (HM Treasury, Bank of England and the FSA) have rolled out a programme of market-wide exercises and benchmarking

Case Study Financial Services Authority

**John Milne,
Head of Business Continuity
Management**

John Milne, Head of Business Continuity Management at the Financial Services Authority, believes that promoting good practice rather than setting stringent directives is the key to achieving the objectives of resilience and market confidence. "We believe that firms' own self-interest, from the point of view of survival and competitiveness, is the main driver," he adds. As an indication of the effectiveness of the approach he cites the response to the FSA's benchmarking project and the annual market-wide exercises which have simulated terrorist attacks and a flu pandemic.

In terms of guidance on resilience issues, the FSA handbook states simply that all regulated entities must have a business continuity plan in place, that it should be appropriate to the size and

nature of the firm, and that it should be reviewed and tested on a regular basis. "We regulate such a wide range of firms that it is difficult to be more prescriptive," says Milne "there is no one-size-fits-all solution. We consider business continuity as an operational risk and therefore primarily an issue of good housekeeping. It is the responsibility of the board". He confirms that the FSA currently sees no need to take a more directive approach, unlike in the US where firms deemed to be significant market participants, are required to have three back-up sites located at progressively greater distances from their main operation, as well as specified recovery times.

Instead the FSA promotes good practice through benchmarking, its annual exercises and the publication of its Business Continuity Management Practice Guide. The preferred approach is to work in a voluntary and cooperative way with firms which allows them greater latitude to tailor their response arrangements to suit their particular business circumstances.

The initial benchmarking exercise, involving the major systems and global players, comprised 1400 questions and took three months to complete. However Milne points out that a smaller version of the questionnaire has now been produced – dubbed Benchmarking

Lite – comprising around 250 questions. This is aimed at a wider group of firms and acts as a self-audit and self-assessment tool. "It enables firms to identify weaknesses in their plans; they can then look at what the BCM Guide offers in that area of weakness by way of standard and leading practice which they can implement in whatever way is most appropriate to their business to promote enhanced resilience," says Milne. "Taken together we believe that Benchmarking Lite and the BCM Guide offer firms an effective self-help 'toolkit' in their efforts to improve their resilience and recovery capabilities."

"Our programme of annual market-wide exercises highlights that interdependency is the key aspect to business continuity. In Financial Services, more than any other sector, your own business continuity is only as good as that of your counterparties". In 2007, the FSA will re-benchmark the firms that took part in the 2005 assessment and Milne is confident that levels of resilience will be shown to have improved.

"The industry is working closely with us to develop and pilot the benchmarking and market-wide exercises," says Milne. "We are also very encouraged by the level of interest shown in our self-help toolkit since we made it available in late 2006."



Contact us

If you would like to discuss any issue,
please contact:

Rick Cudworth

Global Service Leader,

Business Continuity

Tel: +44 (0)12 1232 3888

e-Mail: rick.cudworth@kpmg.co.uk

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon the information without appropriate professional advice after a thorough examination of the particular situation.

© 2007 KPMG LLP, a UK limited liability partnership and a member firm of the KPMG network of independent member firms affiliated with KPMG International, a Swiss cooperative. All rights reserved. Printed in the UK.

KPMG and the KPMG logo and registered trademarks of KPMG International, a Swiss cooperative.

Designed by: Mlytton Williams

Publication name: Living on the Frontline

Publication no: 306166

Publication date: March 2007

Printed on recycled material