BANK OF ENGLAND

Speech

"Contingency Planning and Systematic Stability"

Speech given by

Alastair Clark, Executive Director, Bank of England

At the Association of Corporate Treasurers, Birmingham

18 April 2002

Introduction

The title of this session is "Creating shareholder value in a period of economic uncertainty". We could perhaps debate whether the present environment is exceptionally or merely averagely uncertain; but the events of 11 September certainly added some additional dimensions to the uncertainty. In any event, I want to say a few words this morning about one aspect of uncertainty, or rather about one aspect of the response to it – that is contingency planning and disaster recovery and, given where I come from, particularly from the point of view of the financial sector.

What exactly, you might ask, is the Bank of England's interest in this? It is several fold.

The Bank pre-1997 - and this remains true under the new regime introduced in 1997/98 - has three fundamental purposes. We call them our Core Purposes and they are: monetary stability; financial stability; and promoting the effectiveness of the financial sector in meeting the needs of the rest of the UK economy. Proper contingency planning is relevant to all three. On the monetary side, because it can help to minimise the real economic cost of any major incident. In terms of financial stability, because the capacity of companies as borrowers and lenders, and of financial firms as intermediaries, to cope with disruption is critical if the financial system is to keep functioning. And finally, because effective contingency planning is part of ensuring that the financial sector can do its job properly, and at reasonable cost, in support of the rest of the economy.

Background

Let me start with a few general points.

First – widely recognised but worth repeating – **the US and global financial systems**, despite the scale of the destruction on 11 September, **kept going pretty well**. Much of the credit is due to individuals and private firms, but it also belongs to the US public authorities and especially to the Federal Reserve. There is a great deal to learn from what did and what did not work in New York, and those lessons are now being absorbed. That said, we clearly need to guard against simply "fighting the last war". The nature of any future incident is very likely to be different – it might, for

example, involve widespread and sustained denial of access in the event of a biological attack, or corruption of IT systems through a "virtual" attack.

Second, although 11 September has increased the focus on **contingency planning**, it **is not of course a new issue**. All companies, whether in the financial sector or more generally, have plans for dealing with threats to "business continuity". It is part of good business practice in mitigating operational risk; and for regulated firms, regulators have routinely monitored and assessed the robustness of their procedures for responding to shocks. What perhaps is new is the perception of the immediacy, and even more the nature and scale, of the threat; and this has led to some rethinking about the basis on which risk assessments are made. In the financial sector, for example, it has highlighted the consequences of incidents which disrupt a large number of firms at the same time, or have an impact simultaneously in different places.

A critical issue for firms and the authorities is therefore **what sort of contingency it is sensible or realistic to plan for** – how "big" an event contingency arrangements should be designed to handle. At one end of the spectrum, there are clearly incidents which may be highly disruptive and damaging for individual firms but which are unlikely to have any significant knock-on effects. For contingencies at that level, any response is very largely a matter for the individual firm. At the other end of the spectrum, there are contingencies which are prospectively so serious that maintenance of the financial system in anything but a rudimentary form - or, for that matter, most other sectors of the economy - is unlikely to figure high on the list of priorities. This would most obviously be the case with, say, a nuclear attack. What point to aim for between these two extremes is perhaps impossible to say. There may, however, be a slightly different approach - namely to focus on the elements, the "building blocks", of a response applicable in a wide range of circumstances. Even then it may make sense to test out these building blocks under a range of scenarios, to see at what points and in what ways the contingency arrangements are likely to come under strain.

Third, **much of the burden and cost of contingency planning inevitably falls on private firms** – as it should, given that they have a clear commercial interest in business continuity. **But contingency planning is also very much a joint effort by the public and private sectors**. The public sector has a major part to play, notably in maintaining the physical infrastructure (power, water, telecoms, transport, etc) and in trying to ensure compatibility of approach across different

sectors. In the UK, there is a well-developed civil contingency apparatus coordinated by the Cabinet Office which aims to ensure coherence in the overall response to a major incident.

Fourth, the - sometimes derided - **preparations for Y2K proved fortuitously to be of value in the quite different context of 11 September**. Although the nature of the Y2K threat, the predictability of its timing, and so on, all distinguished it from what happened on 11 September, there were nevertheless some important similarities. Both involved, actually or potentially, widespread disruption to firms and infrastructure; both were accompanied by uncertainties about the exact nature of the threat; both involved the economy as a whole not just the financial sector; both raised issues about the coordination of public and private sector action; and both raised the question of what central banks and regulators needed to do to maintain market functioning. Although Y2K turned out, for whatever reason, to be something of a non-event, the preparations nevertheless ensured that many of these questions had received serious consideration.

One final point. 11 September demonstrated that **wider financial problems**, not just operational problems, **can arise in the aftermath of a major incident**. These included, for example, the sudden withdrawal of insurance cover, and the sudden downturn in air traffic with the associated cash flow and credit issues for airlines. These demanded an urgent response but have also had longer-term consequences. Moreover, there may now be greater uncertainty about exactly where the financial hit from a major incident will be felt, given the growing capacity of markets to slice up and redistribute risk. And beyond all this, there was - and to some extent still is - uncertainty about the wider impact on economic prospects nationally and internationally. In fact, so far, these have turned out to be less serious than many originally expected. But clearly much depends on whether 11 September turns out to have been an isolated incident or the first of a series.

Some specific issues

So much for general background. Let me comment briefly on some specific issues we have identified in our own post-11 September discussions. When I say "our own discussions" I am referring primarily to the financial sector and to the work of the joint Standing Committee, set up as part of the new institutional arrangements introduced in 1997 for maintaining financial stability, and comprising representatives of the Treasury, the Bank and the FSA.

The first issue – which has emerged as perhaps the single most important concern – is **communication**. "Communication" here means communication amongst relevant firms, infrastructure and service providers, regulators, central banks and finance ministries both before and after an incident has occurred.

In advance, the main objective is to exchange information about who is doing what, and to try to ensure that plans are comprehensive and consistent. This is not altogether straightforward, because there are sometimes questions of commercial confidentiality and sometimes also of physical security. To try to help the process along, the Standing Committee has organised meetings with market practitioners and has set up groups to consider particular aspects of contingency planning. We have also launched a web site for sharing information, at present on a limited basis but with the intention that it will shortly "go public".

After an incident, the main challenge is simply to maintain the means of communication if normal channels have been disrupted. What, for example, are the relative strengths and weaknesses of telephone land lines versus mobile networks? What part might satellite phones play? And what about internet and e-mail links, which had a critical role in New York.

Communication also raises the question of <u>what</u> information is likely to be useful. The potential range here is too wide to set out in detail now. But it certainly includes, for example, information about how to get in touch with key people, about the immediate financial position of firms, and about who has the necessary powers, and discretion to exercise them, both within firms and in relation to markets. Much work is underway to provide clearer answers to these questions.

A second key lesson of 11 September was the importance of **resilience in the physical infrastructure generally**. Apart from the obvious issues relating to phones and IT, there were problems with, especially, power and transport. Individual firms' business continuity arrangements tend to assume that the physical infrastructure will be in place and functioning. The experience in New York demonstrated that this will not always be the case. The relevant suppliers - in many cases now in the private sector - have themselves been reviewing their contingency arrangements. One of the key questions is how far their facilities are vulnerable to "single points of failure". Another is

how to make sure that consumers have access to relevant information about the infrastructure, while recognising the confidentiality and sensitivity of some of that information, and its potential value to terrorists.

By way of illustration, let me say a word or two about activity in the UK in the area of telecommunications. The main networks have been reviewed and the conclusion is that the Public Switched Telephone Network is fundamentally resilient; similarly the internet. The mobile network also seems to be physically resilient, outside the immediately affected area; but, as New York demonstrated, it is vulnerable to overloading. Availability of telecoms is crucial for business resumption in the financial sector, and a group has therefore been established to examine telecom issues specific to the sector and to propose guidelines on best practice. One of these is likely to be that firms find out whether they genuinely have parallel routing for their communications – which is not ensured by having two different telecom service providers.

A third important message coming out of 11 September is the need to consider **continuity of staffing** as well as continuity of physical systems. Most directly – to put it brutally – this is the question of how to continue operations if key personnel are killed or incapacitated, or if, for some reason, they cannot be contacted. This issue arose in a stark form for several firms on 11 September. There is probably no entirely satisfactory strategy to cope with this threat; the expense and the motivational difficulties of maintaining "shadow" management and operational capability are likely to be too great. Nevertheless there are some approaches which, at least for major international firms, may provide some degree of protection. They may, for example, be able to switch activity from one centre to another when staff in both are involved in similar if not identical areas of business. Key infrastructure providers may correspondingly need to maintain several operating sites, or at least maintain one or more "hot" standby sites, with local, adequately-trained staff. Whatever the approach, perhaps the real point is that the need to address the issue of staffing continuity is now much more widely recognised.

A fourth key consideration, and in many ways the most obvious, is the **adequacy** or otherwise **of firms' physical contingency plans.** The issues here are complex. In the financial sector, and I am sure more widely, regulated firms – certainly all major regulated firms – are required to demonstrate that they have realistic arrangements for coping with various kinds of operational risk, of which

destruction or inaccessibility of key operational sites is clearly one example. Ensuring, so far as possible, that these arrangements work - not just in principle but also in practice - is essential. There were some instances, following 11 September, where back-up sites or systems did not operate as planned. But as well as these issues relevant to individual firms, there is a question about whether the financial system as a whole is likely to prove robust. How far might the plans of individual firms, which taken on their own look entirely sensible, turn out to be inadequate or inconsistent when looked at in aggregate. Might the whole, so to speak, be less than the sum of the parts? One aspect of this is the issue of "co-dependencies" – single points of failure affecting many different parts of the system. In the context of contingency sites, this would arise if, for example, several different firms had contracted with a single supplier for access to a particular site – which clearly could not be occupied by all of them at once. Choosing a contingency site also gives rise to the dilemma of whether it is best located close to the primary site, more easily accessible but more likely to be affected by an "event" which takes out the primary site, or remote, and prospectively therefore inaccessible even if it remains intact.

Drawing once more on the experience of 11 September, my fifth point is the need for clear guidance on the **practical aspects of market functioning** in circumstances of crisis, and on what adjustments to normal practice are acceptable. In New York in many cases these adjustments were discussed and agreed by the relevant market associations and notified to the regulators. This approach has many attractions, because practitioners specialising in a particular area are more likely than anyone else to know what is important, and what will work and what will not. Market associations need, however, to have sufficient standing so that their conclusions, even if not binding in a strictly legal sense, are nevertheless accepted in practice. This approach also, of course, requires that market associations with the relevant capacity exist for each of the major markets, whether for sterling liquidity, foreign exchange, equities, government bonds or whatever. Contingency planning is already a well-established feature of exchange traded markets; the Bank has been working with the major OTC markets to ensure that corresponding procedures are in place.

Finally, there is one aspect of contingency planning which I should flag as having a special interest for central banks. One of the reasons why financial markets were able to keep going so well after 11 September was the Fed's policy of providing very large amounts of liquidity to banks which found that their normal payment flows were disrupted. Without this, there is no doubt that the financial and economic repercussions of the attack would have been much more serious. **The arrangements for**

providing this **liquidity** raise a number of issues, however, for example where firms operate in a variety of currencies in a number of different countries, and also and more importantly because of the risks associated with unsecured lending. Lending on this basis became almost unavoidable on 11 September, given that the assets which would normally be used as collateral were unavailable with the disruption to the custody and securities handling machinery. Judgements on the risks and the benefits in such circumstances can probably only be made on a case-by-case basis. But with the amounts prospectively involved, they are judgements which central banks, and indeed other market participants, are bound to take extremely seriously.

Closing remarks

Let me finish with just three additional observations.

First, I think we are all aware of the need to move beyond analysis and discussion to action. And there has already been a good deal of action by various of the parties involved in contingency planning. Keeping everyone in touch with what is going on is a challenge in itself and one of which the Treasury, the Bank and the FSA are all very well aware. And in the financial sector, perhaps as much as any other, it is essential that the international aspects of contingency planning are recognised.

Second, some of the issues raised are technically or in terms of the prospective cost/benefit balance, difficult to call, and further work is needed before any sort of plan can sensibly be decided. There is no point in diverting effort into a half-baked proposal which quickly turns out to be inadequate or unworkable. That is a major part of what we are involved in now.

Finally, I recognise that much of what I have had to say may be more directly interesting to financial firms than to companies generally. But I believe some of the issues are of wider relevance; and I hope that in any case you will draw reassurance from the fact that we are, in a variety of ways, trying to ensure that the financial sector, on which you all depend, is adequately prepared against any future disruption.