Roger W Ferguson, Jr: A supervisory perspective on disaster recovery and business continuity

Remarks by Mr Roger W Ferguson, Jr, Vice Chairman of the Board of Governors of the US Federal Reserve System, before the Institute of International Bankers, Washington, D.C., 4 March 2002.

* * *

Good morning. I would like to thank the members of the Institute of International Bankers for the opportunity to speak about disaster recovery and business continuity. This topic has been receiving a great deal of attention at the Federal Reserve and in the financial industry as a whole since September11. It's fair to say that following September 11, we (bankers and supervisors alike) have a renewed appreciation of the meaning of the term "emergency preparedness."

The Federal Reserve and other regulators, both here and abroad, have been analyzing the aftermath of the terrorist attacks with a view toward strengthening the overall resilience of the financial system. This work has benefited from discussions with leading members of the financial services industry over the past several months. In this presentation, I want to give you a flavor of the ideas and issues under review.

Since many of you had first-hand experience of the impact of September 11, I do not intend to dwell on the details of the operational breakdowns and related challenges that faced institutions in lower Manhattan. Suffice it to say that, through a fortuitous combination of existing plans, people, systems, and tools and an extraordinary level of cooperation among market participants, the financial system recovered remarkably quickly from the tragedy. However, we cannot assume that the same combination will always work in our favor, and therefore, regulators and the public have a strong common interest in learning from our horrific experience of September 11.

What did we learn?

Let me review some of the key lessons that we believe have emerged from September 11. First, business continuity planning at many institutions, although improved by Y2K preparations, clearly had not fully taken into account the potential for wide-spread disasters and for the major loss or inaccessibility of critical staff. Some firms arranged for their backup facilities to be in nearby buildings for quite legitimate efficiency and convenience, and, as a result, lost both primary and backup sites. Very few firms planned for an emergency that would disrupt multiple sites in an entire business district, city, or region.

Second, business concentrations, both market-based and geographic, intensified the impact of operational disruptions. Besides the geographic concentration of financial institutions within New York City, some critical market functions, particularly in the clearing and settlement of funds, securities, and financial contracts, rely on only a few entities. When even one of those entities has operational problems, many market participants feel the effects.

Moreover, significant telecommunications vulnerabilities resulting from concentrations became evident when failures affected numerous institutions, both within and outside lower Manhattan. In fact, Federal Reserve staff were personally involved in setting priorities for the restoration of key telecommunications circuits supporting the financial services system during the week of September 11.

Third, the events of September 11 graphically demonstrated the interdependence among financial-system participants, wherever located. Though organizations located outside the New York City area were affected much less than those within it, many felt the effects of the disaster. The difficulty customers and counterparties had in communicating with banks, broker-dealers, and other organizations in lower Manhattan seriously impeded their ability to determine whether transactions had been completed as expected. In some cases, some customers were affected by actions of institutions with which they did not even do business, for example, when funds or securities could not be delivered because of operational problems at other institutions.

In fact, during the week of September 11 liquidity bottlenecks at times became so severe that the Federal Reserve needed to lend substantial amounts directly to institutions through the discount window, besides providing billions more in payment system float on uncleared checks, and through

open market operations. We kept our payment systems open until nearly midnight each night that week as institutions attempted to clear out payment queues. Heightened liquidity needs were not limited to domestic financial institutions. The Federal Reserve set up swap lines with other major central banks to allow foreign banking organizations to obtain liquidity directly from their own authorities, to prevent U.S. liquidity imbalances from being transmitted overseas.

Most important, we learned, as a result of these interdependencies, that contingency-planning decisions made by an individual institution may affect not only the safety and soundness of that institution but also the safety and soundness of other institutions and, indeed, the very functioning of the financial markets. As a result, we believe that coordinated discussions of sound practices for business continuity involving the financial industry and regulators are an important part of our response to the events of September 11.

Steps financial institutions are taking

Let me turn to steps that institutions are taking to improve their own preparedness and business continuity planning. September 11 may lead to changes in institutions' planning for emergencies, as well as changes in their ongoing operations. In addition to a range of tactical steps, such as enhancing security measures, updating communication plans, and strengthening real-time data backup, institutions also are making some interesting strategic choices.

For example, many institutions use a traditional model of business continuity that is based on an "active" operating site with a corresponding backup site, often with separate sites for data processing and for business operations. This strategy generally relies on relocating staff from the active site to the backup site and on maintaining backup copies of technology and data that are up-to-date.

In the traditional model, backup capabilities are ensured through periodic testing. Even so, maintaining the effectiveness of backup sites, staff, and systems that are not routinely used for production is often difficult. For example, during the week of September 11, many institutions found that disaster-recovery plans of particular business lines were not always accessible or up-to-date, and sometimes the backup and primary sites used different hardware and software versions. Finally, the assumption that key personnel could be relocated was not always well founded.

In contrast, some institutions are now moving toward a "split operations" model, in which two or more active operating sites provide backup for one another. Each site can absorb some or all of the work of another for an extended time. For banking organizations with nationwide operations (particularly those that have grown through mergers), such sites are often hundreds of miles apart. For international firms, routine workloads can be shared among sites in different countries or different continents. This strategy can provide almost-immediate resumption capacity, depending on the systems supporting the operations and the communications and operating capacity at each site. The strategy also addresses many of the key vulnerabilities of the traditional model. For example, technology must be kept current at all active operating sites for normal business operations to proceed.

At the same time, the split-operations approach can have significant costs, in terms of maintaining excess capacity at each site and of adding operating complexity. This approach may be more suited to some types of business activities, such as trading, clearing, and settlement, than to others. Other business-continuity models may be able to provide a high degree of resilience. Over time, technological change will significantly affect the range of business continuity strategies and, importantly, their relative costs and benefits.

Whatever operating model they chose, financial institutions clearly are reassessing the range of scenarios they need to address in their business-continuity planning. Such scenarios posit effects on business operations over much broader geographic areas than previously imagined (such as a city or a metropolitan area) and involve consequences that could harm or significantly disperse an organization's critical employees.

Institutions are also exploring methods to provide a greater diversity of telecommunications services and to eliminate points of failure. Contract provisions and audit oversight of telecommunications vendors may heighten attention to this critical vulnerability. At the same time, many recognize that overcoming telecommunications vulnerabilities will be extremely difficult given the current physical infrastructure. In the longer term, establishing diverse telecommunications methods (such as Internet and wireless) and moving toward wider geographic diversification of operations may address these vulnerabilities. Industrywide discussions with telecommunications providers may help institutions to

avoid some of the vulnerabilities exposed on September 11. Some institutions are reexamining arrangements with disaster-recovery vendors because they have found that these vendors' "first-come, first-served" policies mean just that.

Testing of backup plans is also receiving renewed focus. Testing is seen no longer as a compliance issue or an item on a checklist but as a critical part of business operations. In the wake of September 11, many market participants found themselves operating from their backup sites and discovered they had problems connecting and communicating with the backup sites of other displaced entities. As a result, financial institutions now seem receptive to coordinated testing between backup facilities.

In addition, several public and private-sector initiatives have begun to examine the issue of coordinated crisis management communication. Overall, I believe that financial institutions are addressing many of the key vulnerabilities. In large part, the market will demand this. Customers increasingly require assurances that their financial institutions' operations will continue as expected even in the event of a disaster. We need to maintain our focus on this issue even as the harsh memories of September 11 fade. We must also find ways to make business-continuity planning more consistent, more coordinated, and more transparent across the industry. With that in mind, I will discuss some of the steps that regulators are taking.

Steps regulators are taking

The Federal Reserve and other financial services regulators want these lessons to be addressed before the next disaster, whenever and whatever it may strike. First, we are talking to our industry colleagues about appropriate sound practices. However, I would stress that we still have a lot to learn from financial institutions and from experts in business-continuity planning. No one knows for certain which threats (both man-made and natural) we are most likely to face in the coming years. We have much less experience modeling and predicting these operational risks than we do credit or market risks, and indeed some threats may be too idiosyncratic to be modeled at all.

As a result, a prudential supervisory model appears preferable at this time. Through the routine supervisory process, we are talking to institutions about the robustness of their disaster-recovery planning but are stopping short of setting detailed regulatory standards at this point. Although I anticipate that we will issue updated supervisory guidance and examination procedures for business continuity before long, I am not certain that we want to approach this issue with a checklist. In this process, we are working closely with other regulators, including the other federal banking regulators and the Securities and Exchange Commission.

Cities and regions outside New York City are not without risk and also need to consider reasonable threats, both man-made and natural. I am therefore pleased that many institutions in those cities and towns, like their colleagues based in New York City are seriously considering updating and implementing business-continuity plans.

Institutions also need to define their targets for recovery from a disaster in a consistent manner. Although in practice, expectations for recovery time may differ depending on the scenario, some critical functions, including those safeguarding and transferring funds and financial assets, are so vital to the domestic and global financial system that they arguably should continue with minimal, if any, disruption, even in the event of a major regional disaster. Clearly, all institutions need to plan to continue serving their customers in a major disruption, and supervisory standards have required them to do so for many years. In addition, it is increasingly clear that the operational resilience of the largest institutions in key markets needs to reflect their systemic impact across the financial sector. Expectations should be highest for institutions whose activity can significantly affect other institutions, such as major clearing and settlement entities, and institutions that act as financial "utilities" in some of their functions.

However, we need to balance competing issues. We have an ongoing interest in the safety and soundness of individual institutions, as well as in systemic financial stability. But we also recognize that, even though the largest nationally and internationally active U.S. and foreign banking institutions have a key role to play in financial stability, they also participate in a competitive marketplace. Thus, we need to be careful not to create undue burden on a handful of institutions.

Conclusion

Six months after September 11, much has been planned and achieved, but we still have much to do. We must sustain the current drive to minimize or eliminate the vulnerabilities I have discussed. We must view September 11 as a wake-up call to improve the resilience of financial markets and institutions. We cannot afford to ignore the lessons learned.

I ask for your cooperation in what we view as a partnership. We were there for those who needed us on September 11 and in the days that followed, and we will be there again, if necessary. But we also look to financial institutions to conduct an honest appraisal of their vulnerabilities--or to listen to our appraisal of them in our routine supervision over the institutions' U.S. operations--and to take the necessary actions to remedy any significant operational weaknesses and deficiencies.

I wish us all the best in this endeavor.