Keynote Address
by
Steve Malphrus, Federal Reserve
on
"Telecommunications and Financial Sector Resilience"
IEEE CQR International Workshop
June 9, 2006

I am delighted to be your keynote speaker today. The telecommunications industry has a long history of providing reliable communications services to consumers, and has consistently proven to be an effective recovery agent in times of natural and man-made disruptions to the critical infrastructure. This workshop is a good example of the industry's commitment to maintaining and improving the quality and reliability of communications networks, systems, products and services.

The inclusion of the financial sector perspective as a theme of the workshop is appropriate because the financial sector, which transacts business around the globe on a virtually 24 x 7 basis, is keenly dependent on telecommunications -- and information and communication technology more broadly -- in order to do business. Accordingly, the financial sector should be monitored carefully for signs where the telecommunications infrastructure may need to be strengthened and for cues where new services and features may be warranted. The financial sector is the most electronic of sectors in the United States.

Today I would like to highlight a series of issues pertaining to financial sector resilience. Financial sector resilience is an area the Federal Reserve cares strongly about. We believe that in order to meet the financial and economic needs of the country – and assure continued confidence in the United States financial system – the financial sector must recover rapidly from disruptions – whatever the cause or scope. Thus, when I talk about resilience, I am not focusing solely on taking necessary and appropriate precautions to avoid or prevent disruptions…operational disruptions involving business processes, systems, and people occur every day, some more evident to the public than others…I am talking about anticipating disruptions (whatever the cause) and making preparations to recover critical operations, at least sufficient to wind down business activities in an orderly manner.

Achieving and sustaining resilience, though, raises complicated issues. There are steps financial firms can take to increase their resilience to operational disruptions. Even before the modern

banking and securities statues and regulations were adopted, the financial industry was expected to meet a very high standard of care in the handling of customers' money, securities, and confidential financial information. Thus, financial institutions have a long-standing culture that emphasizes strong internal controls and physical and cyber security, and this culture has been vigorously reinforced by the regulators through regulations and guidance. I.T. has been an integral part of the financial industry since the 1960s and the industry has strived to achieve reliable, efficient and secure information systems to streamline business processes. The financial sector understands its dependency on technology, and the complexities of managing the related operations, reputation, and legal risks involved. This has resulted in a more comprehensive approach to managing I.T. risk and business continuity planning: one that goes beyond recovery of data and recognizes the importance of recovering and resuming business operations.

But we also rely on other elements of the critical infrastructure such as telecommunications and power to do business. I am hard pressed to envision a payment or other financial transaction that does not occur in some part over telecommunication circuits. Thus, the resilience of the telecommunications infrastructure is of vital importance to our ability to recover. But, the financial sector can influence improvements in telecommunications resilience to only a limited degree and the need to assure the resilience of the telecommunications infrastructure is an issue the financial sectors worries about. Moreover, the evolving structure of the next generation network (NGN) and the rapid shift to IP-based business processes superimposes a whole new set of risks – in addition to obvious benefits -- that each of our sectors and participating organizations must understand and balance appropriately. Today I will reference a set of work streams involving the public and private sector that are designed to address the resilience of the financial system and the telecommunications infrastructure in the United States.

NS/EP

By way of background, I want to explain how the telecommunications system meets certain national security requirements in times of emergency. In 1963, legislation was passed that created the National Communications System (NCS), an agency that was charged with developing programs to provide priority communications for critical government functions during emergencies. In 1984, the National Security and Emergency Preparedness (NS/EP) capabilities of the NCS were broadened and an interagency group (currently twenty-two federal departments and agencies) was formed to help coordinate and plan NS/EP priority telecommunications services. Our telecommunication companies agree to provide these services to the government, as well as to private sector entities that provide critical emergency services or a meet a national security criteria and who are sponsored by an NCS member agency There are five broad categories that serve as guidelines for determining who may qualify for NS/EP programs: (1) national security leadership; (2) national security posture and u.s. population attack

warning; (3) public health, safety, and maintenance of law and order; (4) public welfare and maintenance of national economic posture; and (5) disaster recovery.

NS/EP programs provide priority for landline (GETS) and wireless (Wireless Priority Service) voice communications. GETS and WPS increase the probability of completing a call in times of heavy usage. I used GETS to call the First Vice President of the Federal Reserve Bank of New York on the morning of September 11 and it worked.

Another program - the telecommunications service priority or "TSP" Program -- provides priority treatment for the Nation's most important telecommunication circuits in times when service vendors may be overwhelmed with requests to restore existing services or establish new services. The TSP program authorizes and requires service vendors to provision and restore TSP assigned services before meeting the needs of other customers, and provides vendors with legal protection for giving preferential treatment to NS/EP users over non-NS/EP users. As a matter of general practice, telecommunications service vendors restore existing TSP services before provisioning new TSP services. TSP worked very well on 9/11 and the days following to restore financial services. Fortunately in the financial sector we had registered a large number of our critical circuits for TSP priority.

The federal financial agencies have extended access to the GETS/WPS/TSP programs to additional financial market participants that support critical NS/EP functions in financial markets including critical funds transfers systems (wholesale/large-value payment systems); securities and derivatives clearing and settlement systems; supporting communication systems and service providers; key financial market trading systems and exchanges, as well as others. Circuits of key institutions to their back-up sites are also now required.

Financial System Resilience

For the financial system, resilience has systemic as well as safety and soundness aspects for individual institutions. Let me give you some details on what I mean by the term "systemic." Every day approximately 3.4 trillion USD payments occur over two wholesale payments systems -- that is when banks make payments to each other on behalf of customers. To put these numbers is perspective, our Gross Development in the United States in 2005 was $12.4 trillion. GDP is the value of goods and services provided in the United States over the entire year…this means that the wholesale payments systems process GDP every four days. Moreover, these numbers do not include payments related to completing transactions in the corporate securities markets, or the futures or derivatives markets.

At the systemic level, therefore, we are most interested in assuring that the financial infrastructure – the payment and settlement systems, and systems supporting those activities -- are robust and able not only to recover critical operations after a major operational disruption,

but also able to resume processing new transactions as soon as the markets begin trading again. I am referring to the *Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System* issued by the Federal Reserve, the Comptroller of the Currency (which regulates national banks) and the Securities and Exchange Commission in April 2003. The sound practices focus on achieving the capability to recover clearing and settlement activities from a wide-scale disruption within the business day on which a disruption occurs. A wide scale disruption, by its very nature tends to involve the disruption or destruction of the critical infrastructure as well as of financial market participants. Accordingly, the sound practices look to systemically critical or important financial market participants to maintain geographically dispersed backup sites from which they can recover operations sufficient to complete material open transactions. Geographic dispersion is the most effective strategy for recovering from disruptions that are caused by local or regional disruptions to the critical infrastructure.

The sound practices apply to organizations and firms that process transactions and make payments – they act as "financial utilities" and have to meet the highest standards. They also apply to banks and broker dealers with large market shares in certain financial markets, such as the corporate and government securities markets, foreign exchange markets and wholesale payments. The financial utilities have substantially implemented the sound practices. And, the agencies are assessing implementation by firms that were identified as having "significant" market share (i.e. maintain at least five percent of the dollar value). The agencies would like to see all covered firms substantially complete implementation no later than year-end. The three agencies recently provided a status report of progress on achieving the goals in the sound practices report to the Congress.

The Financial Sector more generally is subject to business continuity planning expectations that are considerably more robust than they were prior to September 11. The Federal Financial Institutions Examination Council (made up of U.S. banking regulators) issued revised guidance on business continuity and Information Security for all depository organizations following September 11. The guidance calls on baking organizations to incorporate the risk of a wide scale disruption into their Business Continuity Plans. Likewise, following September 11, the SEC issued a policy statement on principles of business continuity planning for trading markets, including a next-day business resumption goal and has recommended that the securities markets conduct independent reviews and risk assessments of the controls for automated trading and information dissemination systems. All broker dealers are subject to regulatory requirements with respect to establishing and maintaining business continuity plans and setting appropriate recovery time objectives. We understand that most broker dealers, and other securities markets participants refer to the recovery time objectives to the trading markets as a benchmark for their business resumption plans. Most recently, both the banking agencies and the SEC have called on

institutions to ensure their business continuity plans address the pandemic flu threat. I shall talk more about the Avian flu threat later.

While the financial sector has long been a leader in matters of business continuity and information security, it has become even more proactive in identifying and responding to the evolving field of operational risk. The industry, trade associations, and the Financial Sector Information Sharing and Analysis Center (the FS/ISAC) have worked together to build robust communication and coordination facilities and actively share best practices. I believe that the NISCC ("NICEY") provides the same services as our FS/ISAC – although I understand that it serves all sectors.[1]

Over the past few years, the financial services industry has sponsored a series of "street tests" that have had broad participation and have been useful in demonstrating that connectivity can be established from backup sites to trading markets, financial utilities and counterparties. The most recent test involved corporate and government securities and futures industry participants. Another very ambitious test is scheduled for this October. Accordingly, while no one can anticipate every event or crises, I believe that the financial sector is better positioned to recover from operational disruptions than it has ever been. As you might expect financial firms have worked closely with their telecommunication providers when planning tests.

Telecommunications

Yet the resilience of the financial sector is dependent on the critical infrastructure and in particular telecommunications – or "information and communication technology" (ICT) as it is now referred to in literature reflecting the ongoing transition to the next generation network.

Telecommunications is the single greatest external vulnerability for the financial system and other elements of the critical infrastructure. Often, there is no viable substitute, particularly for the transmission of data which is critical to the operation of the financial system. Compare the sector's experience during September 11 (no connectivity to markets and market participants, with the resulting market closures) with the August 2003 U.S. power outage (markets and market participants were able to continue important activities using backup power).

In the U.S., the telecommunications infrastructure has a number of significant vulnerabilities, in particular the concentration of facilities (circuits, vendors) within the "last mile," especially in metropolitan areas. In the United States, the transition over the last 25 years from AT&T to a highly populous telecommunications industry that competes on cost has caused a dramatic

[1] *NATIONAL INFRASTRUCUTURE SECURITY CO-ORDINATION CENTRE.*

increase in sharing facilities and similar cost reduction arrangements. As a result, while the telecommunications infrastructure remains highly reliable, it may be significantly less resilient.

After September 11, the Federal Reserve and an industry organization called BITS Financial Services Roundtable asked the National Security Telecommunications Advisory Committee (NSTAC), a group that is made up of industry CEOs and reports directly to the President, to examine the resilience of the telecommunications infrastructure.

We asked the NSTAC to consider short term steps to address resilience (such as heightening protection for high level switches, COs, conduits, and cell towers) as well as longer term approaches (such as developing strategies to increase the resilience of the telecommunications infrastructure where vulnerabilities are most significant; considering alternative methods of transmission; and encouraging R&D in areas such as the transition to packet switching). One of the ways the financial institutions believe they can provide resilience to operations is to establish a physically diverse twin for key telecommunications circuits. Accordingly, we asked the NSTAC to focus on the "diversity issue." With NSTAC's agreement, the Association for Telecommunications Industry Solutions (ATIS) and the Federal Reserve subsequently sponsored the National Diversity Assurance Initiative (NDAI) project, which was recently completed. Both the financial sector and telecom providers learned some important lessons which you will be hearing in more detail later this morning. Without stealing any thunder from Doug Langley's presentation, the results indicate that the telecommunications infrastructure cannot currently provide a physical diversity solution for critical circuits.

The NDAI Report has broad relevance for the telecommunications sector as well for other sectors. It provides information and terminology that can be used by organizations supporting critical National Security/Emergency Preparedness services to better understand the telecommunications infrastructure supporting their business needs in a multi-carrier environment. And, it specifically recommends that other industries beyond the financial sector -- such as power and transportation – whose critical missions depend on telecommunications should evaluate their risks in regards to telecommunications continuity and take the necessary steps to mitigate those risks. The report also recommends that there should be a follow-up work stream to identify the requirements for providing an automated end-to-end diversity assurance solution in a multi-carrier environment. We agree and strongly support this next step.

However, we also believe that there are steps that can be taken now to reduce telecommunications operations risk, though the establishment of geographically dispersed sites, the use of sonnet rings, and the like (risk-based diversity). And, we hope discussions during today's sessions can lead to the offering of creative, resilient and cost effective approaches that

provide measurable improvements in the resilience of telecommunications to critical infrastructure providers and other significant telecommunications customers.

Cyber Security and Information and Communication Technologies (ICT)

The financial sector depends on technology to do business and in general it appears that our sector is holding its own in the area of cyber security. We have a robust ISAC, although software security and patch management is a serious ongoing issue, as is the insider threat. At the retail bank level we are seeing widespread use of online banking services by consumers who are finding these services convenient and cheap. However, as a wider range of financial services and transactions become available over the internet, the potential for cyber fraud and theft also increases. Today of the approximately 8,800 insured depository institutions in the US approximately 8,360 (95%) have websites and approximately 7,100 (85%) of them permit transactions such as payments.

Likewise, the Fed has been implementing an internet based product that allows banks to make wholesale and ACH payments via a Virtual Private Network transported over the internet. The key to security is a controlled environment with both the Fed and customer banks taking responsibility for security.

In response to the evolving threats, last October, the Federal Financial Institutions Examining Council issued guidance on "Authentication in an Internet Banking Environment." Institutions are advised to conduct risk assessments that focus on high-risk transactions (e.g., includes third-party funds transfers and electronic bill payment systems) and develop appropriate security measures such as multi-factor authentication.

U.S. Initiatives

As I mentioned earlier, telecommunications is recognized in the U.S. as having a significant national security aspect, and there are numerous federally-sponsored agencies and organizations that provide oversight and input to telecommunications providers. Because communications – voice and data – are now conveyed via multiple channels, the focus has broadened considerably to include ISPs, hardware and software developers, and wireless and satellite telecom companies, in addition to the more traditionally organized telecom service providers. As I am sure you are aware, wireline, wireless, and internet protocol networks are converging at a rapid rate. This convergence is referred to as the Next Generation Network or NGN. While it is clear that the NGN will offer significant improvements for communications such as increased bandwidth, interoperability with various intelligent devices, and a wider range of applications, many of the new features of the NGN present challenges for ensuring security and availability for important

types of communications (for example, government communications or payment instructions versus an order for a new video game).

My comments in this area will reference reports and recommendations recently issued by two groups. The first is the National Reliability and Interoperability Council VII (NRIC), which is an advisory group, sponsored by the Federal Communications Commission and made up of primarily of private companies as well as some government agencies (I participate on behalf of the Federal Reserve as one of the financial sector's representatives). The NRIC recommends best practices for the communications industry. Last year the NRIV VII issued best practices in a number of important areas including emergency/911 services, homeland security, wireless and public data network services, broadband, and cyber security. The second group is the NSTAC, which I referred to earlier in connection with circuit diversity. In March, the NSTAC issued a *Next Generation Networks Task Force Report*.
http://www.ncs.gov/nstac/nstac_publications.html#2006

NRIC Cyber Security Recommendations

In December 2005, an NRIC Focus Group issued a set of technical best practices pertaining to cyber security for telecommunications companies, many of which also are applicable to commercial enterprises and technology vendors. Looking forward, the group recommended that future cyber security focus groups consider developing best practices for voice over IP; identity management in the network environment; wireless security; messaging security; and to help protect against blended attacks, fraud and other abuse. I wonder though, whether the telecommunications sector can play a more prominent role in assisting the public by filtering out viruses and other types of cyber attacks launched across their networks.

The focus group also identified several cyber security issues that are important enough to be addressed at the national level but do not lend themselves to Best Practices. For example the focus group suggested that Internet Protocol Version Six -- which federal agencies are expected to implement – has the potential to help solve the security problems present on current IP networks. But the focus group also suggested that implementations of IPv6 could be as problematic in security concerns as IPv4 and could introduce *new* security problems not yet envisioned. Some of my staff have similar concerns. In fact, hybrid IPv4/IPv6 networks seem to be increasing the complexity of the network, and this alone may introduce new vulnerabilities. The NSTAC NGN Task Force Report, however, had only positive thinks to say about IPv6. It states that IPv6 provides fundamental benefits over IPv4, including a vastly increased number of available IP addresses, more efficient routing infrastructure, better security implementation, and increased mobility while maintaining existing connections. These differing opinions make it

even more difficult for the relatively lay persons who are charged with managing their own or their firm's ICT systems in this rapidly changing environment.

NGN

As you know better than I, the NGN is not one all encompassing network; for the foreseeable future, the NGN will be based on a set of interconnected individual networks. A key question for all of us is: are we ready for the NGN? I am interested in your reactions because I see some issues that suggest that the NGN may become a reality, perhaps before we are ready. Users (business, financial firms, government agencies, and consumers) of the network see the internet as a very cheap vehicle for operating a whole range of intelligent devices. However, it is important to balance cost savings and apparent robustness against what could be a significantly increased risk environment. The increased scale, scope – and character – of the NGN presents a host of unknown dependencies, interdependencies and vulnerabilities that we may not fully understand and therefore may not be able to manage proactively. I would like to see a broader discussion between the financial sector and the network providers (telecom and ISPs), and applications and operating system developers regarding the evolving structure of the NGN. My quick list of essential features includes: survivability, broad platform support, and strong network authentication, priority for NS/EP traffic, international connectivity, reliability/availability, and affordability.

However I am told that users will be expected to incorporate encryption and other security services at the application layer. One needs to ask if it is acceptable to have the network security functions devolve "to the edge"? Given the multiplicity of intelligent devices on the network, it is unlikely that end users (companies, financial firms, agencies, and consumers) will be able to reasonably manage security and address the multitude of other network issues on their own.

Interestingly, the NRIC cyber security focus group identified similar issues pertinent to the NGN with respect to the "transport" layer of the Internet Protocol. Their list of national issues includes the fact that some layers of the IP protocol suite do not implement any security controls and are easily violated. The focus group warned that as more and more critical applications are deployed on an unsecured IP protocol suite, the risk for outages, hacker attacks and other sorts of malfeasance are certain. It expressed concern that work to achieve a secure IP protocol needs to be better organized and, even then, it will be several years before a proper upgrade of the suite can be engineered, developed and deployed. The focus group strongly recommended that NRIC establish a focus group to look into the problem of cyber security in IP protocol suites. It stated that this should be a high priority due to the continued aggressive deployment of IP as the preferred transport protocol for critical infrastructure.

In my view, it is not in anyone's best interest to push responsibility for security and compatibility to end users. We need to work with network and applications developers to understand and agree on the necessary attributes of the NGN. But who will lead the effort?

The NGN Task Force Report discusses the NGN solely in the context of assuring that National Security/ Emergency Preparedness priority programs are supported by the NGN is a seamless manner. Its recommendations though would benefit all NGN users. The report calls for development of a common operational criteria that assures reliable and secure end-to-end service; development of a cohesive domestic and international policy to harmonize protocols for NS/EP incident response in the international NGN environment; and for additional work in the areas of identity management and incident management.

End-to-end reliability in the NGN requires coordination of multiple connected networks, linked both physically and logically via common operational criteria accepted and enforced among adjacent networks. But development and enforcement of a common operational criterion is an international issue involving both the public and private sectors…

What do you see as your role in the evolution of the NGN? What do you think is the appropriate role for other sectors – and for governments and consumers? How can we assure that the critical attributes I mentioned are built into the NGN? I encourage you to review both the recent NTSAC "Next Generation Networks Task Force Report" and NRIC focus group paper on cyber security best practices -- and to move the network in the right direction.

Pandemic flu

Finally, let me briefly address the new threat on everyone's mind today, the pandemic flu. As I indicated, the agencies have recently issued supervisory guidance. I believe that the pandemic flu threat can be addressed within our Business Continuity Plans. The threat is different however because of scale, duration, the doctrine of social isolation and high rates of absenteeism. These differences must then be addressed in our plans. Because the financial sector is highly automated much work that is done in the office can potentially be performed at home via conference calls and remote access to information resources. However, in developing a telecommuting strategy the following must be considered:

- While wide area networks will likely handle the increases in telecommuters, the most variable and overall limiting factor is capacity in enterprise networks.
- There is potential for an increased level of cyber attacks and hackers targeting enterprise networks and home computers. We should expect that the fraudsters and hackers will exploit an expansion in telecommuting.

- Tasks for our voice and data communications systems administrators will increase and they will be more vital than ever in maintaining our ability to operate. We need to think carefully how we will support their work.

Conclusion

My goal today was both to thank the telecommunications industry for the service you have rendered in times of greatest need: natural and man-made disasters. I hope my remarks today are also useful and thought provoking. My goal was to provide you with the financial sector overview of issues pertaining to telecommunications that are most relevant to the continued resilience in the U.S. financial system. Individually and collectively, you can continue to help.

Thank you. I look forward to today's discussions.