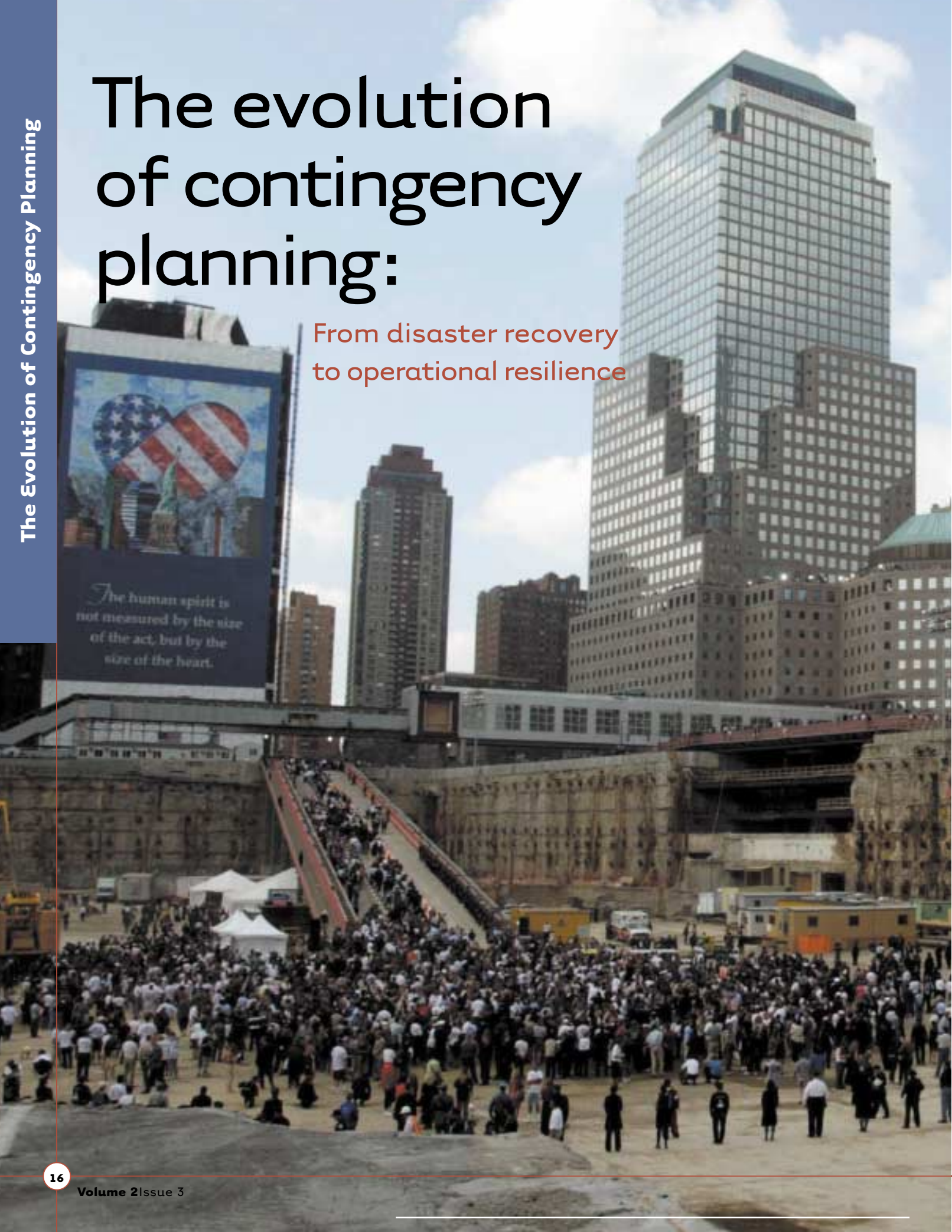
The evolution of contingency planning:

From disaster recovery to operational resilience



It's actually the relentless application of technology over the past decade and not the events of September 11 that have driven ever more interest in information availability and operational resilience. SunGard is a global leader, with over 10,000 Availability Services customers, many of whom are from the financial services industry, says Till Guldimann, vice-chairman, SunGard

Since 9/11, the word "disaster" has become inextricably linked to terrorism. Renewed attention is being given to recovery after a catastrophic event to ensure financial services firms can get back up and running quickly and to minimize systemic risks. This attention is crystallizing the need for a new perspective on the challenge of disaster recovery. The fact is that financial services today are managed and delivered through an amalgamation of networks – tightly intertwined and electronically linked – and the system's vulnerability is a source of increased concern. We have become dependent on the network; therein lies the real threat to firms and the financial system as a whole.

The old paradigm was redundancy – backup, backup, backup. The new one is resiliency – keep your operations humming and ensure your node on the financial network remains "online". The contingency challenge has shifted from disaster recovery – cleaning up and getting back to work after a cataclysmic event – to operational resilience – designing your enterprise to operate effectively right through a disruption.

This new vulnerability isn't a consequence of terrorism; rather, it's driven by the relentless application of technology to the business of finance. Technology has transformed the money markets, and simultaneously generated substantial new risks for every market participant. Because technology is vulnerable – to natural disasters, to terrorist attacks like 9/11, and to cyber-terrorism in the form of the rapidly emerging epidemics of computer bugs, worms, and viruses.

Based on data from Swiss Re, Chart 1 (*right*) shows that, while natural disasters continue to take their toll – particularly in terms of human life and particularly in the developing countries – man-made disasters like terrorist attacks are getting more expensive.

Two examples: 1985 and 2001

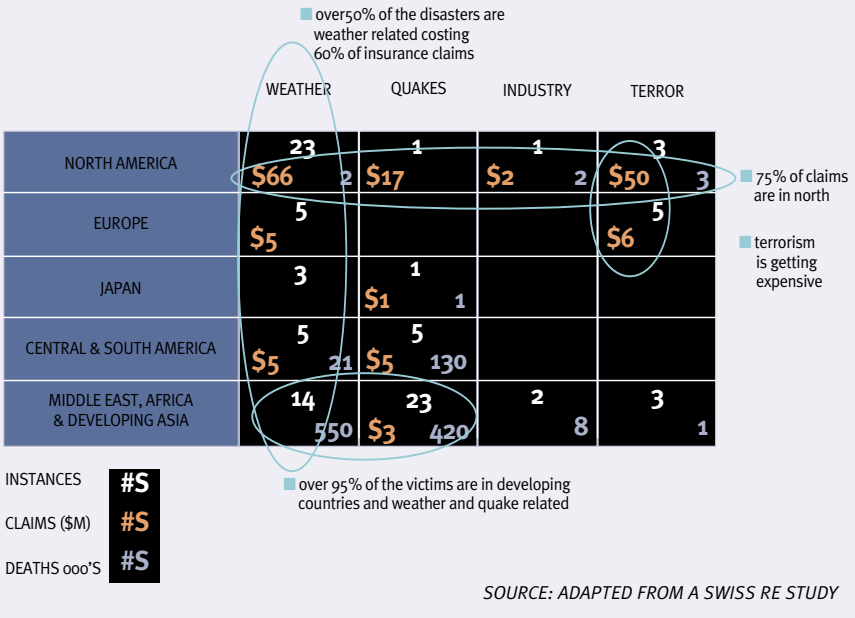
To highlight the new reality, compare a severe market disruption in 1985 to the one caused by the attack on the World Trade Center a year ago. The earlier event demonstrates the risks posed by a software problem at a single firm; the more recent one demonstrates the risks of highly interdependent networks.

On November 20, 1985, the clearing operation of The Bank of New York (BNY) handled more than 32,000 Treasury security trades for the first time. This record volume triggered a software problem, preventing the firm from delivering treasuries to buyers. The next morning was settlement day, and BNY began accumulating undelivered securities, which had to be financed by borrowings at the discount window of the New York Federal Reserve. BNY had to borrow a staggering $23 billion by the end of the day. The following morning, with the software still malfunctioning, the Fed told dealers not to deliver more treasuries through the affected clearer, which led to a broadening of the disruption. Fortunately, the software was corrected later that day and clearing normalized.

The lesson: because of a high concentration in the market for clearing services, a single malfunction in a single firm's system led to an expensive crisis and highlighted systemic risks in the U.S. Treasury market. Not incidentally, no systems backup could have prevented the problem.

Now compare this to what happened in the same market on September 11, 2001. Again, BNY is an active player, clearing more than half of all U.S. government securities transactions. Volumes are far greater, and the bank's systems are far more robust, with multiple data centers and recovery sites pri-

Chart 1: Biggest disasters 1972–2001 (insurance industry perspective)



SOURCE: ADAPTED FROM A SWISS RE STUDY

marily located in New Jersey and therefore physically unaffected by the terrorist attacks. What is different this time is the critical role of the telecommunications infrastructure handling all the data traffic created by the trading activity. When the network hubs in the World Trade Center were destroyed, traffic was automatically routed to another hub nearby, which happened to be the principal access point serving BNY. The ensuing enormous surge in telecom traffic swamped that facility, temporarily disrupting communications for clearing. Trades stopped being executed and settled; the business shut down.

Even though the bank was physically removed from the World Trade Center destruction, BNY's dependence on the network infrastructure had a profound ripple effect throughout the government bond market.

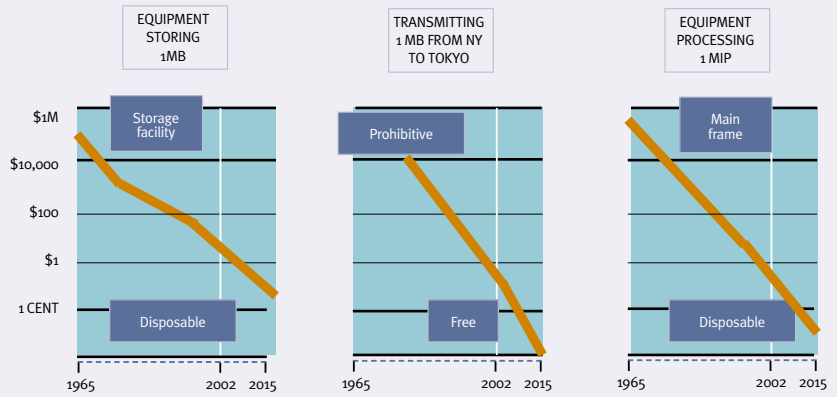
Technological progress and asset growth: drivers of the new reality

To understand today's environment, we must take a look at the most profound drivers of the financial industry over the last two decades: the precipitous fall in technology (hardware) costs and the dramatic rise in investment assets.

In effect, the marginal cost of hardware is going to $0.00, and this has had a huge impact on financial markets. Access to information is cheaper and broader; markets are more efficient; volumes have skyrocketed; and cycles have accelerated. Combined with financial deregulation on a global scale, the result is greater competition, more specialization, and a deeper reliance on network infrastructures.

By any metric you care to look at, the hardware costs of processing, storing, and transmitting information have plummeted, and the trend line is clear: the hardware-specific costs of IT are dropping, essentially to zero (see Chart 2 (*above*)). To cite just one example first reported in *Fortune* magazine (March 1999): six years ago, in 1996, the entire U.S. long-distance telephone capacity was one terabit/second – enough for about 15 million simultaneous phone calls. By 2001, that capacity had increased by a factor of 100 – two orders of magnitude – with the obvious consequence: lower costs and higher traffic.

Chart 2: IT revolution drives global restructuring



If technology has changed the nature of finance, so too has the opportunity created by the massive shift from bank deposits to investment assets. In 1980, bank deposits accounted for more than half of the roughly $2.8 trillion in personal financial assets in the U.S.; by 2000, the assets had grown to $17 trillion, with less than 20% of that money in bank deposits.

Clearly, all these new dollars in securities have to be administered. The growth and competitive frenzy of the asset management industry, coupled with an ever-increasing, technology-driven capability to assimilate and analyze raw data, generated more and more market activity, which in turn generated more and more data, and so on, in a cycle that brought us to the situation as it is today – volumes of trades and information that were unthinkable only a decade ago.

Driven by the need to create and exploit economies of scale, most growing manufacturing industries eventually consolidate. Growing financial markets are no different (the quest for scale and efficiency has certainly generated a lot of mergers). But while scale benefits financial operations, it is inimical to investors. The ability to exploit information and market insights is limited when managing very large pools of assets, simply because the markets are not liquid enough. The liquidity issue forces asset managers to restrict the sizes of investment portfolios, making distribution relatively more expensive as trading costs go down.

Two kinds of players emerge

The result has been a profound evolution in the structure of the financial services industry, with two kinds of enterprises in the ascendant: specialized component producers that do one thing extremely well on a global scale by exploiting technology to achieve economies (in clearing or custody, for example, or processing credit card transactions); and "megabranders" that package a wide range of products and services for a huge global market (exploiting the power of their brands to reach consumers and the power of technology to manage relationships – e.g. Citigroup, Morgan Stanley).

This evolution suggests what the future of the industry will look like in technological terms. Today, the biggest cost component (and therefore the largest cost savings opportunity) is not in processing itself but in the communications between specialized providers, in managing the interactions of all those systems and messages. For specialized component producers, therefore, the best way to cut the costs of production is by moving to straight-through processing (STP). Basically, instead of people reformatting, translating, and relaying the myriad messages associated with transactions, STP means systems talking directly to systems and processing transactions in real-time.

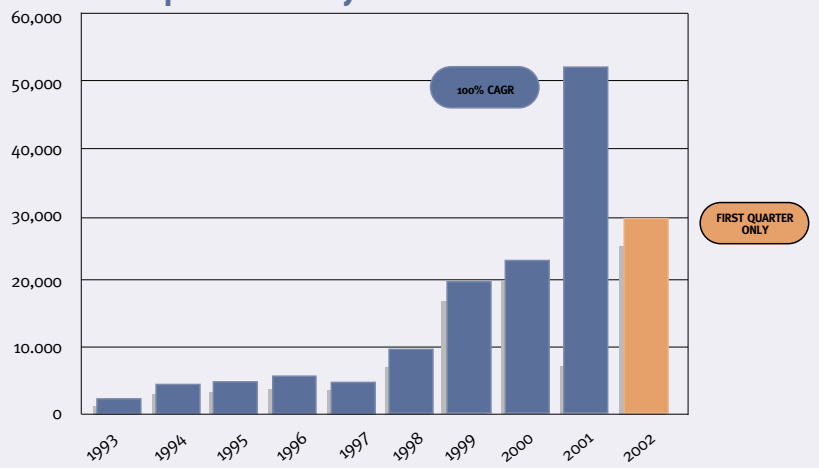
Chart 3 (*right*) illustrates how many parties and systems are involved in executing a hypothetical share trade between an institutional and an individual investor. Each arrow represents a connection between systems – a

communication that often involves an expensive "linkage": a person translating and relaying information. Even straightforward transactions can involve as many as 100 different systems and 200 separate messages.

The adoption of STP, combined with the increased specialization of producers, will result in a monumental shift in financial services processing, from batch to continuous (see Chart 3 (*below*)). Batch processing works well when transaction cycles are long and single firms handle an entire value chain. But as trading volumes increase, transaction cycles shorten, and firms focus and specialize, serialized batch processes become a severe operational bottleneck. The network can no longer be accelerated, while the cost of error-handling goes through the roof.

Implementing STP and continuous processing will require huge investments. One consulting firm, TowerGroup, estimates the financial services industry will spend more than $15 billion to implement STP between now and 2005. A fundamental rethinking of workflows will result in new ways of doing business, and that change is expensive. The silver lining of this challenge is that rethinking workflows enables firms to really exploit the benefits of technology. It is a golden opportunity to make operations dramatically less expensive.

Chart 4: Computer security incidents



Less redundancy, more risk

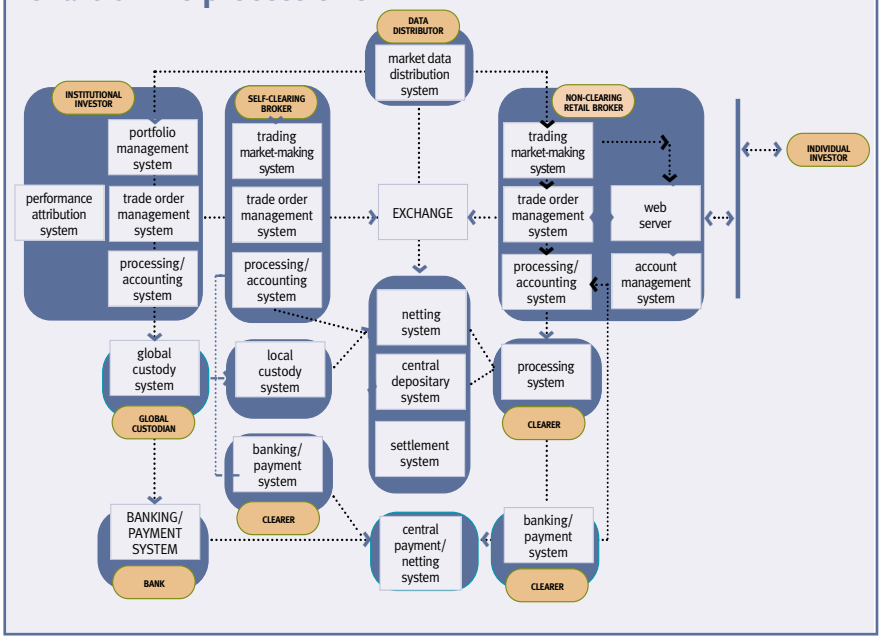
The specialization of finance goes hand-in-hand with consolidation and concentration. In the 1980s, there were 20 substantial credit-card processors; today there are five huge ones. Those five have certainly achieved economies of scale, but they have also squeezed redundancy out of the system, generating new kinds of systemic risk. This is a natural, predictable, but unfortunate byproduct of the invisible hand of the marketplace and its ruthless quest for efficiency – and it poses new challenges for participants and regulators alike.

Indeed, the new systemic risk in the financial industry is no longer characterized by institutions that are "too big to fail", but by institutions that are "too critical to the network" because they are a dominant provider of a highly specialized service. More and more firms are dependent on third-party specialists (consider, for example, the current oligopoly in market data services: Reuters, Bloomberg, and a few others). Furthermore, the increased degree of automation and faster transaction cycles mean that problems anywhere on the network make the whole system more vulnerable. Automation reduces flexibility in responding to emergencies and allows errors to propagate much faster.

These technology-driven issues will continue to evolve the structure of the financial industry in the future, and they create new risk management challenges for managers and regulators. In an environment characterized by highly interconnected, interdependent service providers, network risk becomes paramount when planning for contingencies and disasters. How secure is the network? How redundant is the network? How automated is the network? And, ultimately, who regulates the network when it transcends national boundaries?

While earthquakes and jetliners can have catastrophic effects on financial networks, the bigger and more worrisome threats stem from cyber-terrorism (see Chart 4 (*above*)): computer viruses, worms, and other forms of artificial "life" aimed

Chart 3: The process of STP



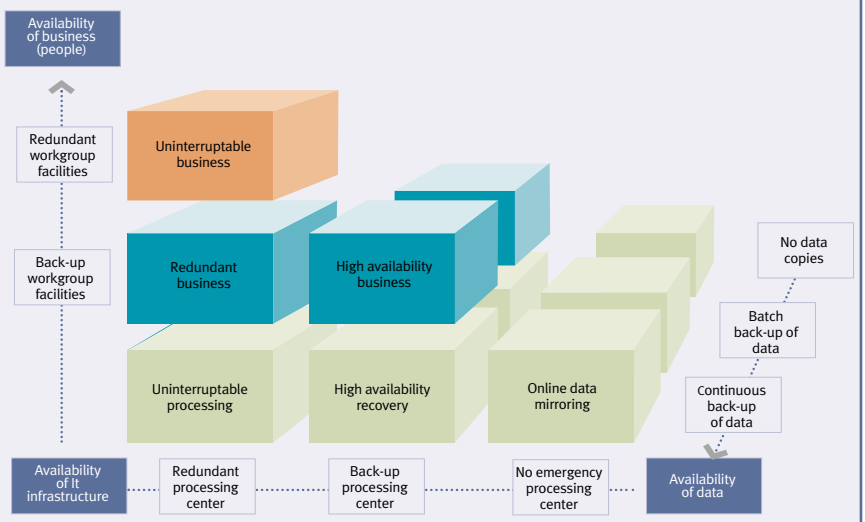
directly at the network infrastructure critical to contemporary finance. According to the CERT Coordination Center at Carnegie Mellon University, which tracks computer emergencies and responses, more than 50,000 computer security incidents were reported in 2001; that number is expected to increase another 100% this year. Losses attributable to viruses in 2001 were estimated at $15 billion. And the threat can only increase as network access points proliferate (think of the potential for viruses to enter the network when every cellphone can access the Web and 802.11b wireless computer networks become truly pervasive).

What to do next

What should you do in this new environment of contingency planning? From a macro perspective, you need to adopt a new distributed architecture for the processes truly critical to your ability to function. A networked operation is far more resilient than a concentrated, standalone operation. A few guiding principles to keep in mind:

- *Identify key businesses and dependencies*. Operating your entire company on a fully redundant basis is not necessary and would be far too expensive. So begin addressing the challenge of operational resilience by identifying which parts of your business need what kind of resilience. Landscaping around your corporate headquarters, for example, will rank low; customer relationship management will rank high. You also need to understand your dependencies on third-party service providers and, most important, whether the third parties you depend on most regard you as critical to their business.
- *Back up processes, not just data*: Under the old paradigm, the focus was on backing up data, but that does nothing to ensure your ability to operate continuously. In the new world, you have to back up data as well as the network and processing capacity; people; and third parties upon whom your enterprise depends. Many firms have back-up data centers and even backup trading rooms, but how many today have their call center operations spread out across the country?

Chart 5:Three dimensions of availability



- *Plan and test for network-related contingencies*. Once you have begun backing up processes and data, you can begin planning for network-related contingencies and actually testing your resilience. The goal should to be remain operating (and to be prepared for substantial – perhaps record – volumes as other financial market participants and their systems come back online). You need to establish clearly defined responsibilities in the event of an emergency and to share your contingency plans within and outside your enterprise (to critical partners, for example). And test your resilience: prove to yourself that your contingency plans will work. (Don't forget to include your firm's senior managers in the tests so they can see firsthand how they'll react and what really needs to be done in the event of a disaster.)

Recovering after the impact of a disaster, whether it is an earthquake in Tokyo, a terrorist attack in Manhattan, or a computer virus unleashed in London, will no longer be sufficient to ensure enterprise safety or systemic integrity. In today's networked financial services economy, financial enterprises must keep going continuously in the event of a catastrophe. Markets can melt down or freeze (choose your favorite metaphor) with great speed, and that speed will only increase as market participants and their systems become more closely intertwined.

We will never be able to make ourselves immune to the human costs of attacks like 9/11, but we owe it to our companies and our industry to make our enterprises as immune as possible to the operational risks posed by them and other threats. Ultimately, it is a matter more of commonsense applications of technology and other resources ("What do I need to do to keep running in the worst-case scenario?") than fancy analytics or sophisticated risk quantifications. Addressing these new risks is vital to the ability of our firms to function and the ability of our system to thrive.

An evolution: From data backup to processing redundancy

As technology becomes more pervasive in the financial business and dependency on technology increases, IT and operations professionals have got more sophisticated about backing up data, from "batch" backups to continuous backups to online data mirroring. Processing capabilities have followed a similar trend line, from scheduled downtime to high availability to uninterrupted processing (see Chart 5 (*above*)). Because data processing is now so deeply embedded in every business activity of practically every employee, protecting the data and the main processing centers no longer assures survival. It is the combination of data, processing and workgroup availability that ensures operational resilience.